NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FROM FOB TO NOC—A PATHWAY TO A CYBER CAREER FOR COMBAT VETERANS

by

Brian R. Gattoni

June 2014

Thesis Co-Advisors:	Steven Hutchison Duane Davis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
FROM FOB TO NOC—A PATHWAY TO A CYBER CAREER FOR COMBAT VETERANS

5. FUNDING NUMBERS

6. AUTHOR(S) Brian R. Gattoni

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Cybersecurity is a growing landscape, in terms of careers and conflict. Federal agencies and private companies are attempting to hire as many qualified cyber professionals as they can to meet the demand of securing this new domain. Veterans are steadily leaving the military for civilian life. Hiring managers need to find qualified employees and veterans need to find post-military employment, but there is no clear path to connect the potential supply with the actual demand.

This thesis researches modern developments in security concepts for forward deployed military personnel and connects those concepts to cybersecurity. A survey of the available jobs in cybersecurity creates another layer of traceability followed by identification of related technical skills identified as potential gaps for potential hires. The gaps help identify available sources of training and certification that can help the veterans fill the gaps. The end result is a matrix that identifies that specific security concepts of perimeter defense for forward operating bases and combat outposts do correlate to cybersecurity roles and that the technical skills required are fully covered by existing training. A roadmap is discussed to synchronize federal efforts around a training program to incorporate the findings into existing recruiting efforts.

14. SUBJECT TERMS Cybersecurity, forward operating base (FOB) security, combat outpost (CO) security, veteran transition, veterans, training, career, transition

15. NUMBER OF PAGES
87

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

FROM FOB TO NOC—A PATHWAY TO A CYBER CAREER FOR COMBAT VETERANS

Brian R. Gattoni
Branch Chief, Department of Homeland Security
B.S., Appalachian State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Author: Brian R. Gattoni

Approved by: Steven Hutchison
Thesis Co-Advisor

Duane Davis
Thesis Co-Advisor

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cybersecurity is a growing landscape, in terms of careers and conflict. Federal agencies and private companies are attempting to hire as many qualified cyber professionals as they can to meet the demand of securing this new domain. Veterans are steadily leaving the military for civilian life. Hiring managers need to find qualified employees and veterans need to find post-military employment, but there is no clear path to connect the potential supply with the actual demand.

This thesis researches modern developments in security concepts for forward deployed military personnel and connects those concepts to cybersecurity. A survey of the available jobs in cybersecurity creates another layer of traceability followed by identification of related technical skills identified as potential gaps for potential hires. The gaps help identify available sources of training and certification that can help the veterans fill the gaps. The end result is a matrix that identifies that specific security concepts of perimeter defense for forward operating bases and combat outposts do correlate to cybersecurity roles and that the technical skills required are fully covered by existing training. A roadmap is discussed to synchronize federal efforts around a training program to incorporate the findings into existing recruiting efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	access control list
ASP	ammunition supply point
AO	area of operations
AV	anti-virus
CAC	common access card
CDD	capabilities description document
CERT	computer emergency readiness team
CISSP	Certified Information Systems Security Professional
CO	combat outpost
CompTIA	Computing Technology Industry Association
COP	common operational picture
DOD	Department of Defense
DoED	Department of Education
DHS	Department of Homeland Security
DOJ	Department of Justice
DMZ	demilitarized zone
ECP	entry control points
ENSA	EC-Council Network Security Administrator
FITSI	Federal Information Technology Security Institute
FM	field manual
FOB	forward operating base
GCIA	GIAC Certified Intrusion Analyst
GIAC	Global Information Assurance Certifications
GS	general schedule
HSAC	Homeland Security Advisory Council
IDS	intrusion detection system
IP	internet protocol
IPS	intrusion prevention system
IT	information technology

LRAS3	Long Range Advanced Scout Surveillance System
MAC	media access control
MOE	measures of effectiveness
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education
NIPRNET	non-secure internet protocol router network
NIST	National Institute for Standards and Technology
NOC	network operations center
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
ORD	operational requirements document
PII	personally identifiable information
PIV	personal identity verification
SIEM	security incident and event management
SOC	security operations center
SORN	system of record notice
TOC	tactical operations center
UMB	University of Massachusetts
VA	Department of Veterans Affairs

ACKNOWLEDGMENTS

I would like to thank my advisors, Dr. Steven Hutchison and Dr. Duane Davis, for their dedication to solid input and keeping me motivated through this process.

I would like to thank my co-workers, the men and women serving in the Department of Homeland Security's Cybersecurity and Communications Network Security Deployment Division. They have been a constant source of encouragement and support for the past 2+ years.

A very special thanks goes to my wife, Rebecca, our three children, and my parents. They have allowed me the time to complete this effort along with a full-time job at the department and coaching every baseball team my children desired to be on.

And, finally, I wish to thank the source of inspiration for my work. As a senior leader and hiring manager in my organization, I've always sought to hire veterans to the mission of the department. I hope that this document allows the search to get qualified veterans into the cyber mission at DHS to improve for both parties.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In order to improve the ability to offer combat veterans an opportunity to continue serving the nation through continued federal service employment as a cybersecurity professional, the federal government needs to create additional training and transition opportunities. At this time, there are no programs designed to inform veterans of the value that their current skills in security can bring to the cyber field or augment those skills through training to address potential technical barriers to success in the cyber domain. These technical barriers may be perceived by the veteran or a hiring manager as insurmountable obstacles to success. Furthermore, while training is available to fill the technical skill gaps, there is no clear path for veterans' transition to federal career roles available in cybersecurity.

B. BACKGROUND

1. The Current Hiring Environment

Cybersecurity is one of the fastest growing sectors in public and private service. Almost every U.S. government department is hiring professionals as quickly as possible. Though the federal hiring process can be cumbersome, it is designed to elevate the highest qualified personnel to the eyes of the hiring manager and it does allow for preference to be shown to specific classes of individuals. Among those groups receiving preferential hiring treatment are veterans, who receive between five and 30 preference points depending on their service. Veterans are entering the civilian workforce at an increasing rate, leaving a military that has been at war for a full decade. This extended state of war has led to several refinements in operating methodology, especially in the area of operating forward operating bases (FOB) and combat outposts (CO) to support counterinsurgency efforts. Many of the skills required to implement these operational innovations, particularly those associated with physical security, conceptually align with high-demand cybersecurity skills.

Some departments are granted special hiring authorities that allow for direct hire, enabling them to avoid competition in order to fill positions quickly. While the process was not designed to undermine veteran preference, it does allow for it. This can lead to a hiring culture that views veterans in a negative light and may foster preconceptions that veterans lack the technical skills necessary to be of service in a cyber mission space.

2. What Can Veterans Offer to the Cyber Mission?

Over the past decade, forward deployed operating units (particularly infantry) have had to adapt to an operating climate unlike any other in the 200-plus years of military history in America. Veterans have had ingrained into them a concept of security that literally kept them alive. This concept of security is broad in its application, and cybersecurity is one of the newer domains for which this concept can be relevant.

This thesis provides a preliminary analysis of the security skillsets of veterans against the skill gaps in cybersecurity for the purpose of designing a manageable path for integration of veterans into the cybersecurity workforce. The focus of the analysis starts with the concepts of security rather than the technical implementations of those concepts. This analysis provides the basis for a proposed training program to transition veterans out of military service into civilian service, while capturing lessons from the field that can be applied to improve security in the cyber domain.

Chapter II reviews documented military regulations and best practices for security of a FOB or CO. Requirements or designs for future improvements to combat outpost security are also discussed. Security concepts identified in these document reviews is then correlated with a real world case example from the investigation into Combat Outpost Keating in Afghanistan. The security concepts identified in this chapter are used again in Chapter IV for comparison with the findings from Chapter III.

Chapter III reviews security concepts of a computer network with examples from federal, military and academic sources of security requirements.

Chapter IV compares the views of combat and cyber with basic security concepts to illustrate the connection between the two domains. Further discussion of federal cyber jobs and their required skill sets is provided to annotate differences in security implementation. Establishing traceability from the skills for cyber jobs back to the security principle learned serving in a FOB or CO will form the basis for training gaps to be discussed in Chapter V.

The link established in Chapter IV between skills required for cyber jobs and skills learned during service at a FOB or CO form the basis for training gaps discussed in Chapter V. This chapter reviews the training goals of several commercial certification programs to determine if those programs fill the training gap established in Chapter IV.

Chapter VI briefly summarizes the preceding chapters and provides a tabular view of physical security and cybersecurity concepts, the associated job skills, and identified training sources for attainment of those skills. Finally, this chapter provides a suggested roadmap for implementation of a pilot program for incorporation of this training into the military transition process.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SURVEY OF PHYSICAL PROTECTION MODELS USED FOR COMBAT OUTPOSTS AND FORWARD OPERATING BASES

This chapter details developments in FOB and CO security models to include advancements in tactics, techniques, procedures and technology used to provide or increase protection for physical locations.

A. FORWARD OPERATING BASE/COMBAT OUTPOST

Over the past decade of military operations, FOBs and COs have been the basic security construct for deployed forces. A FOB is typically a brigade or battalion sized military base constructed within an area of operations (AO) in a host nation. COs are any base smaller than a FOB that are also deployed within the AO. There is a clear relationship of command and communication between FOBs and COs in an AO.

COs are small, reinforced observation posts that can host a company or platoon sized unit plus support personnel to secure and operate the base. They are located in areas of strategic importance to providing security in an AO. COs provide a place to interact with the local population and provide safety for the unit conducting counterinsurgency operations from the base.

U.S. Army Field Manual (FM) 3-24.2, *Tactics in Counterinsurgency,* Chapter 6-30 ascribes the following roles to a CO [1]:

- Secure key lines of communication or infrastructure
- Secure and co-opt the local populace
- Gather intelligence
- Assist the government in restoring essential service
- Force insurgents to operate elsewhere

The Joint Army/Marine Corps Glossary of Operational Terms and Graphics defines a perimeter in context of defense as “a defense without an exposed flank, consisting of forces deployed along the perimeter of the defended area” [2]. The use of the words “without an exposed flank” combined with the idea of a compound is similar to the mathematical definition of the outside edge of an area. In order to not have an exposed flank, the perimeter fully encloses the area to be defended and separates it from the area of the threat. Thus, the defended area is inside the perimeter, and the perimeter consists of a continuous line of demarcation around the area to be defended [3].

In keeping with this generally accepted understanding of the term, the following working definition for "perimeter" will be used throughout this paper: the continuous line of demarcation around a secure physical space that is intended to separate and protect friendly forces from non-friendly and provides a vantage point for security to observe, detect, identify, and engage non-friendly forces.

Field Manual 3-24.2 describes 12 planning considerations for perimeter defense as summarized in Table 1. All of the planning considerations are designed to enhance a perimeter to maximize the defense posture and protection provided to the inhabitants.

Planning Consideration	Example	Planning Consideration	Example
Terrain	Natural obstacles, roads, waterways	**Defense in Depth**	Fall back points, portable obstacles
Host Nation Security Forces	Local police; military forces	**Patrols**	Roaming patrols, checkpoints, dogs
Communication	Internal communications network to TOC	**Maximum use of Offensive Action**	Military tactics to rid area of enemy force
Sustainment	Available landing zones/drop zones for resupply	**Mutual Support**	Overlapping fields of observation, coordinate fire
Protection	Fire response, chemical suppression, medical support	**All Around Defense**	360 degree perimeter
Security	Ground sensors, cameras	**Responsiveness**	Counter attack plans to various scenarios, quick reaction force

Table 1. Planning Considerations for Combat Outpost Security, from [1]

Sections 6-121, 6-122 and 6-129 of the *Offense and Defense* FM highlight the importance of perimeter defense [3]:

- A perimeter defense is oriented in all directions. The prerequisites for a successful perimeter defense are aggressive patrolling and security operations outside the perimeter.
- A major characteristic of a perimeter defense is a secure inner area with most of the combat power located on the perimeter.
- The commander reduces vulnerabilities by: developing reconnaissance and surveillance plans that provide early warning

B. COMBAT OUTPOST SECURITY DESIGN

Figure 1 illustrates a typical defense design for a CO. In this typical design, there are identifiable security concepts that are required for every base.

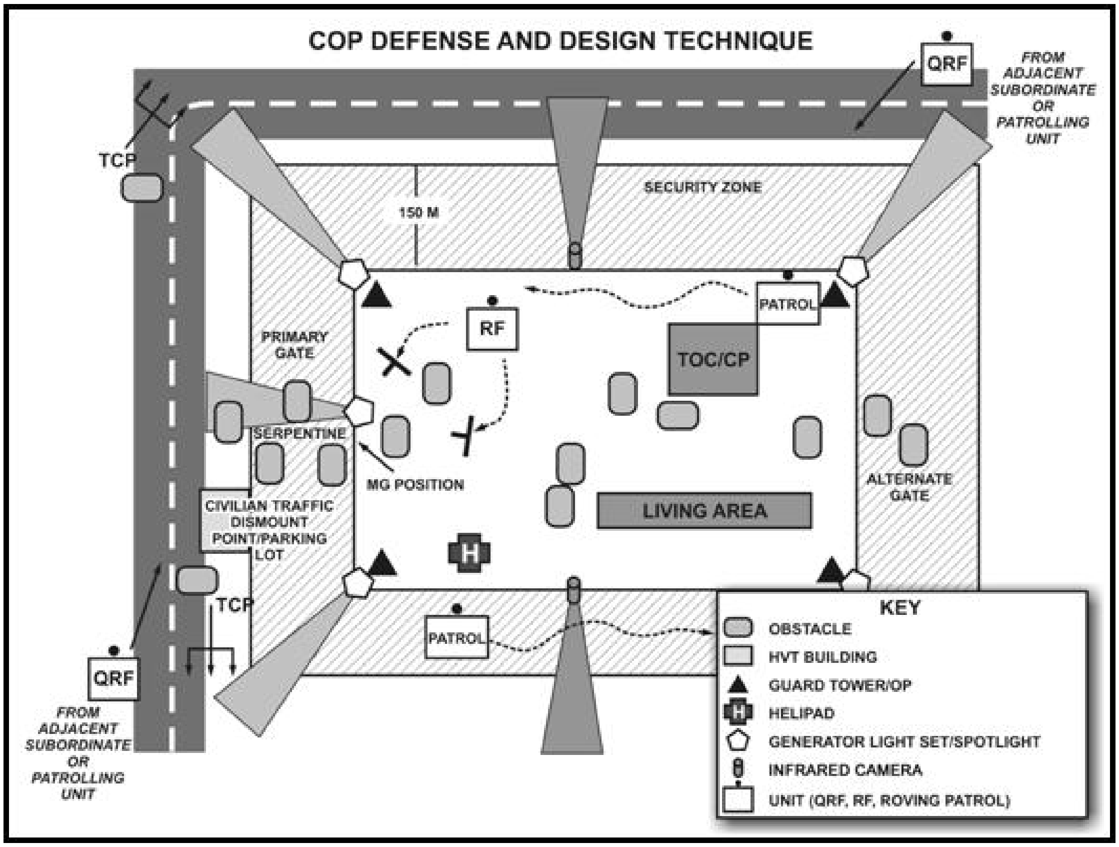
COP DEFENSE AND DESIGN TECHNIQUE
QRF
FROM ADJACENT SUBORDINATE OR PATROLLING UNIT
TCP
150 M
SECURITY ZONE
PATROL
RF
PRIMARY GATE
TOC/CP
SERPENTINE
MG POSITION
ALTERNATE GATE
CIVILIAN TRAFFIC DISMOUNT POINT/PARKING LOT
LIVING AREA
H
TCP
PATROL
QRF
FROM ADJACENT SUBORDINATE OR PATROLLING UNIT
KEY
OBSTACLE
HVT BUILDING
GUARD TOWER/OP
HELIPAD
GENERATOR LIGHT SET/SPOTLIGHT
INFRARED CAMERA
UNIT (QRF, RF, ROVING PATROL)

Figure 1. Typical U.S. Combat Outpost Design, from [1]

1. Control Points

Starting on the left of the figure, traffic control points are placed in all directions of CO approach that allow for the inspection and redirection of vehicles and people. These traffic control points are in place on the side of the CO with the main entrance. The main entrance has an area for a parking lot and a serpentine obstacle that prevents vehicles from approaching the primary gate to the CO itself.

Gates in the perimeter serve as an entry control points (ECP) for the CO. ECPs are the only way in and out of the CO and are the areas where individuals are checked for identification and inspection prior to entering the compound. As a designed ingress/egress point, ECPs are heavily fortified with continuing serpentine positions into the perimeter. There are also reaction forces positioned nearby for armed response as required. Also located at the ECP is a machine gun position to provide protection and overwatch for the manning force at the gate. The security concept employed at traffic control points and entry control points is controlled ingress and egress. Controlled ingress and egress allows for identification and inspection of everything approaching or crossing the perimeter at the allowed points.

2. Perimeter Monitoring

a. Manned

The perimeter requires monitoring at more than just the allowed points of entry. All four corners of the perimeter have a watch tower positioned to give the force a 360 degree field of observation outside the outpost. The 360 degree field of observation extends outward from the outpost into an area security zone 150 meters from the perimeter. The security zone is immediately adjacent to the perimeter and must be observed closely for any threats. The future designs (depicted in Figure 2) for COs call for an area of interest and an area of influence. The area of interest is a 360 degree field extending out to 20 times the length of the perimeter (e.g., 400 meter perimeter has an 8000 meter area of interest). The area of influence is half of the area of interest (e.g., 4000 meters in the previous example) [4].

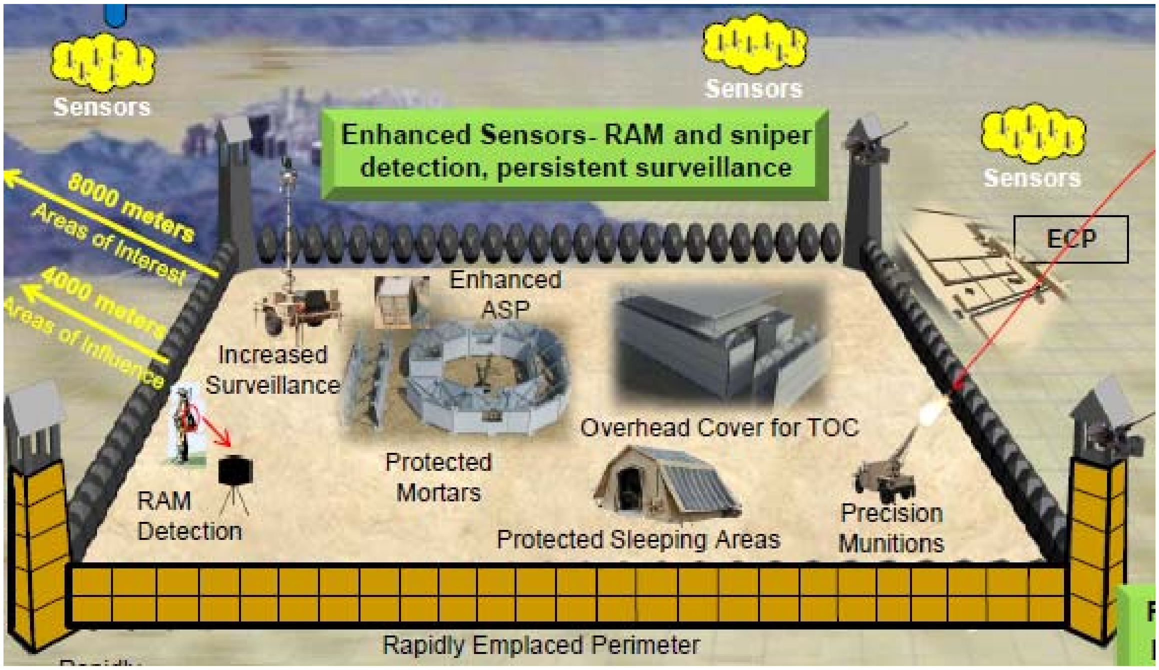

Figure 2. Operational View of Future Force Protection, from [4]

The areas of interest and influence are intended to support observation and detection of movement around the CO without undue burden on the peaceful populace, which is assumed to approach the outpost from the controlled positions and to also give the outpost a wide berth if there is no intent to interact with it. Once a target has entered the area of influence, there must be the capability (in accordance with established rules of engagement) to deter the target from approaching the perimeter in an unsafe manner. Obvious threats (e.g., people or vehicles approaching at high rate of speed while bearing arms) can typically be neutralized with direct engagement. Less obvious threats can be observed and situationally marked for engagement, or issued commands or communications to deter their actions as required.

b. Unmanned

In addition to the manned posts at the corners of the perimeter, the typical design calls for unmanned monitoring capabilities. Figure 1 shows infrared cameras with placements at the center of the perimeter sides that do not have a gate. These unmanned cameras are connected to the CO's Tactical Operations Center (TOC) where their images can be monitored in real-time by a watch officer.

The future CO design of Figure 2 further describes a series of unmanned ground sensors placed throughout the areas of interest and influence. These sensors will also be monitored by the TOC watchstanders and will provide targeting information to remote weapons systems that will use the sensor data to apply fires with precision munitions per the rules of engagement. These capabilities can be threaded together by the TOC to create an automated response capability that increases security and protection to the manned units within the outpost.

3. Buildings

a. Living Quarters

Living quarters are an obvious requirement for any size installation housing military personnel. For FOBs and COs, living quarters present a unique challenge balancing access and protection. Living quarters need to be spaced and protected properly from other buildings, the perimeter, ammunition supply points (ASP), and ECPs. Spacing is critical to enhance protection, but must also support quick response and deployment of troops in the living quarters to their battle stations. The typical design depicted in Figure 1 shows how the living areas are placed far away from the primary gate with obstacles placed between the primary gate and the building to protect from explosions and shrapnel. Future designs incorporate overhead cover to protect from mortars and grenades as well.

b. Tactical Operations Center Command Post

The TOC is the headquarters and office space for the CO. It houses the command, control, communications, and computers for the outpost and represents a high value target for an enemy force. As seen in the typical design, it is protected similarly to the living quarters. Additional obstacles are placed between the primary gate and the TOC. The TOC communicates tactically with each unmanned or automated system deployed in the area.

c. Fuel and Ammunition Supply Points

Fuel or ASPs are required to support the missions of the CO. Fuel supply points are where combustible fuel is stored to run generators, vehicles, and any other combustion engine that requires it. ASPs house the ammunition for every weapon deployed to the outpost, all of which require readily available ammunition. The ammunition supply point must be accessible to the stationary weapons systems deployed within an outpost (i.e., mortar pits). Fuel and ASPs must also be stationed far enough away from the living quarters and TOC to protect those structures in the event of detonation or explosion due to incoming enemy fire. The appropriate minimum standoff distance between structures is an important element of outpost design.

C. REAL WORLD APPLICATION OF OUPOST DESIGN

In July 2006, the U.S. Army established Combat Outpost Keating in the Kamdesh Province of Afghanistan. The CO was located 25 kilometers from the Pakistani border in a basin surrounded by high ground and water. A review of declassified and redacted materials available through United States Central Command's electronic reading room for information releasable under the Freedom of Information Act provides an opportunity to identify the previously described design principles used at CO Keating. Figure 3 illustrates a defensive plan for CO Keating that employs security cameras, and a series of weapons placements to provide 360 degrees of coverage with mortar, grenade, or machine gun [5].

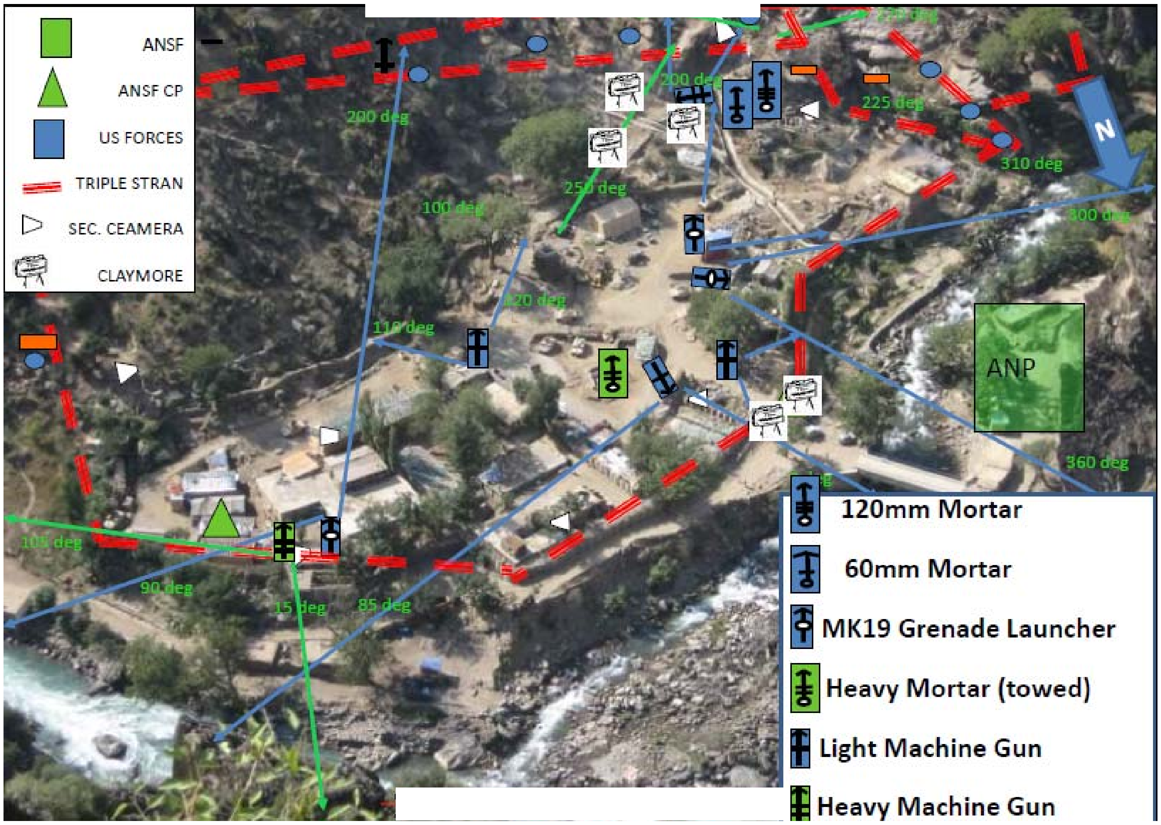

Figure 3. Defensive Diagram for CO Keating, from [6]

1. Control Points

This diagram illustrates the perimeter made of triple strand concertina wire (red line). There was one primary ECP in the perimeter (marked with two Claymore mine symbols). The primary ECP was to the north (right side of diagram) and provides coverage of a main meeting building used for greeting locals and access to a bridge.

2. Perimeter Monitoring

a. Manned

There are examples of manned and unmanned perimeter monitoring capabilities shown in this design. These include three stations manned 24 hours a day and three stations manned twice a day on an irregular schedule or during contact with the enemy to keep any observing enemy wary of the force protection condition at any one time. One of the manned positions was built into the ECP building. The others were two HMMWV vehicles outfitted with the latest Long Range Advanced Scout Surveillance System (LRAS3) capabilities. These tools gave scouts the ability to detect, recognize, identify, and geo-locate distant targets in real-time, day or night [5]. The three irregularly manned positions were trucks outfitted with .50 caliber machine guns or Mk19 grenade launchers. While there were plans to erect towers to replace the vehicles, the vehicles had the capability to reposition themselves within the perimeter to provide coverage for dead space in the event of a firefight [6].

b. Unmanned

Unmanned capabilities are represented by white security camera icons throughout the CO. Each of the cameras was wired back to the TOC for centralized monitoring. Claymore mines can also be considered unmanned capabilities, in that they are designed to explode and kill personnel who engage their tripwire. Claymores were deployed at the ECP to prevent personnel from going around the approved entrance and at the southern end of the perimeter to protect the mortar pits.

3. Buildings

The force protection brief for CO Keating includes Figure 4 and helps illustrate the security design concepts for building location and separation.

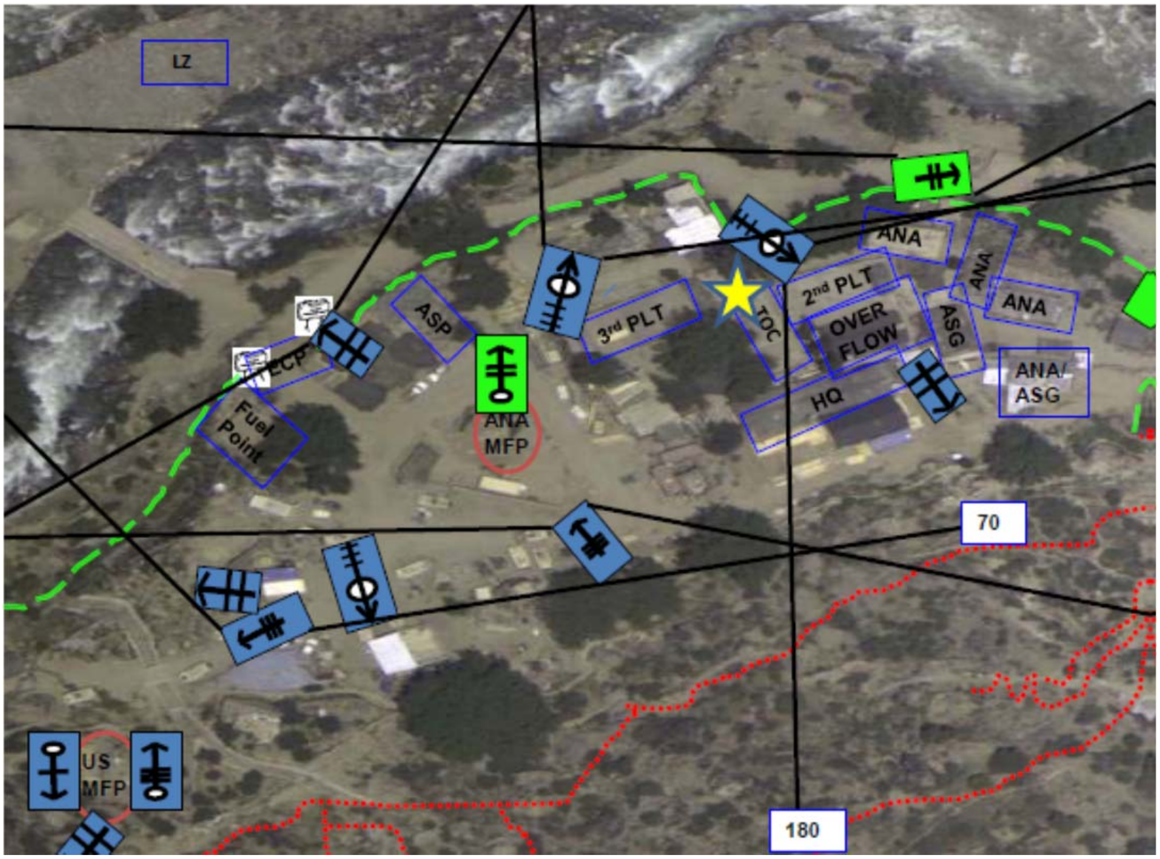

Figure 4. Force Protection Planning Diagram, Zoomed In, from [6]

a. *Living Quarters and Tactical Operations Center*

The TOC for CO Keating was located at the bright yellow star near the center of Figure 4 (for orientation purposes, north is toward the top of this figure). The TOC was separate from, but in close proximity to, the barracks for 3rd Platoon (directly to the west) and 2nd Platoon (directly to the east). There was also an overflow barracks directly south of 2nd Platoon, and a headquarters building. Each of these buildings was protected by several of the 577 Hesco structures within the CO. Hesco structures are modular barriers erected in austere conditions to serve a variety of purposes, but specifically serve as exterior blast barriers for the buildings in CO Keating.

b. Fuel or Ammunition Supply Points

The fuel supply point and ASP could be found near the ECP on the northwest side of the perimeter. The location of these two supply points demonstrate the standoff distance as a defensive concept designed into this outpost. The supply points are located far enough away from the housing and work buildings to protect them from accidental or unintended detonation or explosion. The fuel supply point is located adjacent to the ECP, which would provide for efficient fueling of incoming and outgoing vehicles. The ASP is located where it can support troops requiring small arms ammunition prior to leaving the perimeter on patrol or to resupply the mounted machine guns and grenade launchers within the compound. The precariously distant American mortar fire pit (farthest point southwest) would also be resupplied from this point, illustrating that location priority may not be optimal for every need.

D. CONCLUSION

This chapter identified several security concepts from studying how combat outposts are designed in both doctrine and real life. Clear lines of demarcation in the form of a perimeter provide protection to those within. The perimeter also provides the opportunity to monitor activity approaching the CO and to inspect the ingress and egress of personnel and vehicles. The structures within the CO are purposefully located to ensure a balance of protection and access. Chapter III discusses security concepts in the cyber domain. Chapter IV discusses the application of combat outpost security concepts to cybersecurity.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SURVEY OF CYBERSECURITY PROTECTION MODELS

This chapter examines models developed to secure networks. An examination of network models varied by connectivity, isolation, purpose, and location will support identification of the core security concepts in use in cyberspace, and will provide the basis for comparison with the practice of perimeter defense in military operations.

A. NETWORK PERIMETER DESIGN

Network perimeter designs vary extremely, however many utilize a generalized topology for a secure network perimeter entails three networks in concert separated by two firewalls. The most external network is the Internet, which is separated from the perimeter network or demilitarized zone (DMZ) by a perimeter firewall and a series of switches and routers. The DMZ network is separated from an Internal Network by an internal firewall.

A DMZ network serves to host information that may be exposed to traffic from the Internet. The term DMZ is borrowed from the Korean War term for the area of land that serves as a buffer zone between North and South Korea following the end of military action in the 1950s. A DMZ is a network that operates as a buffer zone between an organization’s internal network and the Internet. The DMZ should prevent unauthorized access to the internal network from the outside. Deployed in conjunction with strong firewall rules and policies, a DMZ is an integral part of a secure network design. The Internal Network hosts information that is only exposed to the Internet through the use of applications or servers in the DMZ. Direct access to the internal network from the Internet should not be possible without the use of proxy services in the DMZ [7].

Figure 5 illustrates a simple view of a general network boundary or perimeter. Network boundaries can be thought of in a linear sense because the data travels over the wire. The internal network may be extremely expansive, but should only connect to the Internet through a boundary configured in this tiered manner. There may be more than one set of internal firewalls allowing access to the DMZ, or there may be multiple DMZ networks. A serious security flaw would exist in a network that had direct access to the Internet from an internal machine; this is what is known as a backdoor in cyber security [8].

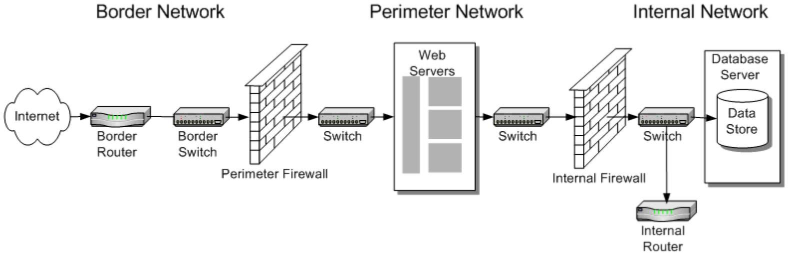

Figure 5. Simplified Network Boundary View, from [9]

Firewalls control the bidirectional flow of traffic between networks. The Internet represents the “wild” and the source of external attacks. Network administrators configure firewalls to allow or disallow traffic based on Internet Protocol (IP) addresses and protocol characteristics, ports and application-level protocol characteristics. Individual traffic types and ports can be configured with a range of rules ranging from “ALWAYS ALLOW” to “NEVER ALLOW” with configurations in between to allow for legitimate or trusted traffic flow.

Within the DMZ, only non-sensitive data and services that are accessible once allowable traffic is passed through the firewall from the public network to the DMZ should be allowed. Public data such as general website information and services such as submission forms and information feeds are examples of data that would be properly hosted inside a DMZ. Sensitive information, such as business or mission databases containing user data or financial data should default to hosting inside the business network and only be hosted in a DMZ for specific cases, such as email servers. Sensitive data that is hosted in the DMZ should not be made accessible directly to the public network.

B. MONITORING

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are typically utilized in the DMZ to monitor and control the flow of data into and out of a network. IDSs and IPSs are software-based systems deployed to commodity hardware or existing networking devices that support the process of monitoring events occurring on a network or computer system. These events are analyzed for signs of security incidents representing violations of security policies.

IDS and IPS devices that investigate network traffic can be preprogrammed with signatures that indicate malicious activity and trigger rules that make decisions based on the characteristics of the scanned traffic. According to the Snort User manual:

> …rules are divided into two logical sections, the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information. The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken. [10]

By targeting inbound and outbound traffic between the Internet and internal networks, IDS and IPS sensors can identify attempted intrusions. Some malware is designed to communicate with command and control networks (e.g., botnets) and therefore create outbound traffic. If this outbound traffic is destined for a known bad IP address or domain, then a signature can be written to identify that activity.

IDS and IPS sensors can also be utilized to monitor internal network traffic and programmed with rules that enforce acceptable use policies and alert security officials in the event of a violation. Internal traffic such as file transfers and database accesses are key areas of interest that can reveal insider threat activity. Each alert requires investigation, but is not necessarily a positive indicator of malicious activity [11].

a. Intrusion Detection and Prevention Systems

An IDS is designed to detect problems and raise alerts. These alerts can be sent to a secondary system that can then take action or aid in analysis. An IDS can be deployed in-line or out-of line with regards to the network traffic. An in-line IDS operates as a pass-through networking device where the traffic comes in and goes out of the IDS. The IDS then matches traffic against the pre-defined signatures. An in-line IDS supports detection of and response to threats in real time at network speed. Figure 6 illustrates the placement of a sensor inline in the DMZ architecture between the internal network and the Internet.

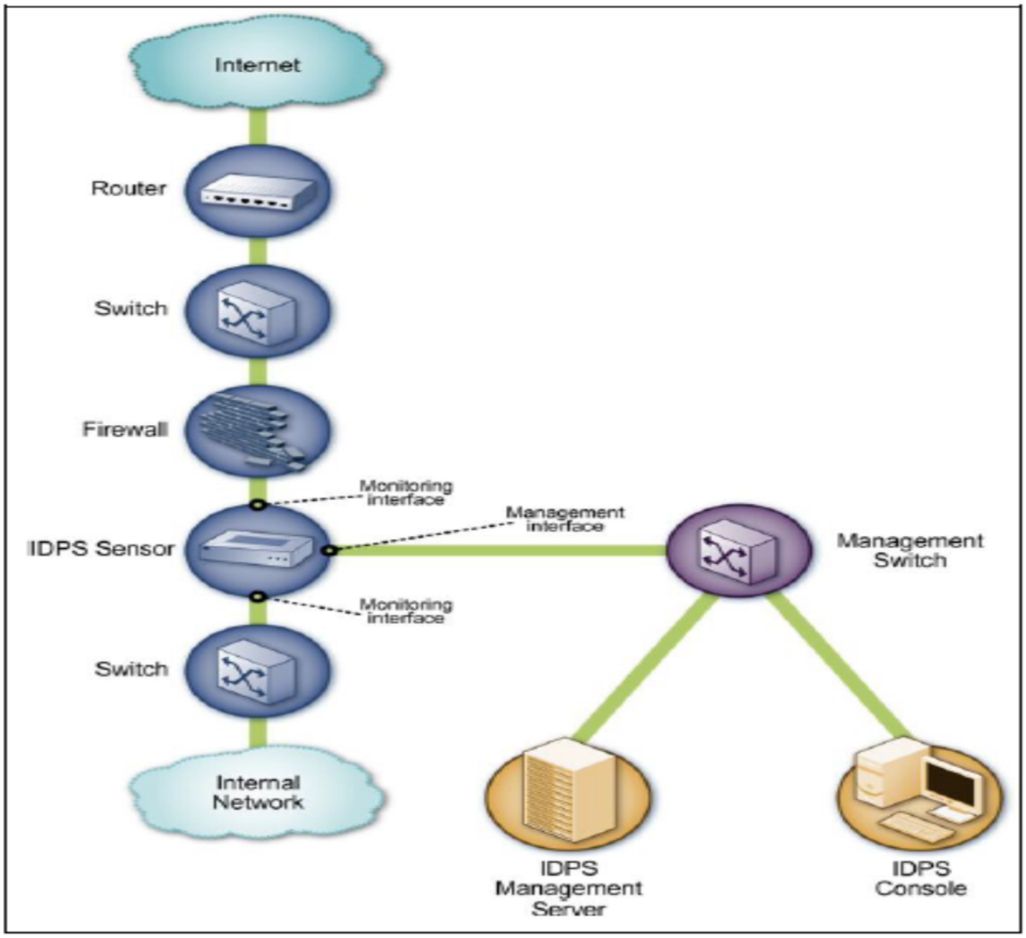

Figure 6. NIST Inline Network Sensor Example, from [11]

An out-of-line or passive IDS is provided network traffic from a mirror or passively monitors network segments in promiscuous mode. The IDS then performs its automated analysis via and populates an alert log. Multiple sensors may be placed at various points in the network path to support aggregation and correlation at a management console. Differences detected amongst various points in the network can indicate malicious activity and support faster identification of attempted or actual network compromise. Network load balancing devices may be necessary to prevent individual sensors from becoming overloaded with traffic at a time of intense activity. Figure 7 illustrates the placement of a passive sensor suite within the DMZ architecture between the internal network and the Internet.

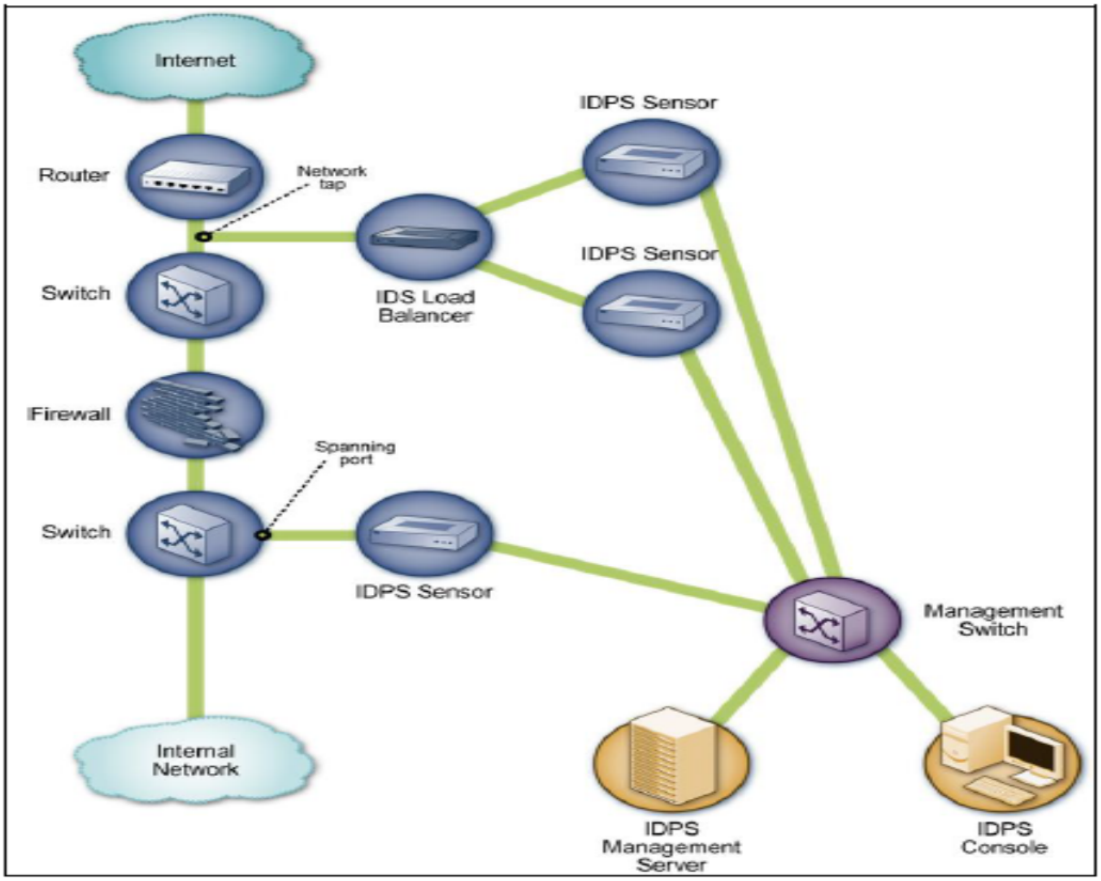

Figure 7. NIST Passive Network Sensor Example, from [11]

IPSs are similar to IDSs, with one main distinction: an IPS can take direct action in response to potentially malicious traffic. As such an IPS is typically deployed in-line with network traffic so that it can prevent malicious traffic from getting to its destination. IDS and IPS devices provide the necessary functions of detection of and protection from adversarial network activity [12].

(1) In-line System Implementation Considerations. In-line systems require consideration of specific factors for placement on the network. An IPS should be placed at the network edge devices within the DMZ to capture data as soon as it enters the DMZ from either the Internet or Internal network. Brief network outages may be necessary when installing an inline device because the end to end connections have to be disrupted to insert the device. There should be no IP addresses assigned to the monitoring interfaces of the sensor device to prevent detection by adversaries during reconnaissance activities [11].

(2) Passive System Implementation Considerations. Not surprisingly, passive systems require consideration of different factors than in-line systems. Passive systems may require load balancing components designed to distribute the traffic amongst several IDS sensors. The traffic from these separate sensors then needs to be combined again at the management console in the correct network sequence to support post-event analysis. The addition of load balancers, switch spanning ports, and network taps requires careful attention at installation. Network taps may be installed with minimal network outage if the interfaces are carefully managed by the network administrators. Passive sensors should also be configured without IP addresses at the interfaces to prevent identification by adversaries [11].

b. Security Incident and Event Management

In addition to the possibility of real-time monitoring, all network systems should be providing activity log data to a central location. A security incident and event management (SIEM) system often provides a key capability for logging systems in a network security operations center. High powered correlation engines designed with business intelligence for security applications can learn the normal traffic behavior on a network and begin to identify anomalies that require further investigation.

SIEM devices offer an indirect method of integrating multiple IDS and IPS devices and capabilities with other network system logs. SIEM devices are designed to support a broad array of data types including firewall logs, antivirus software data, operating system audit logs and application server logs [11]. Each of these data types goes through a normalization process to align and standardize the data types to support correlation of same-type data fields. IP addresses, domain names, time stamps, and other identifying data can be used by the systems or security personnel to develop patterns of normal and abnormal activity. Abnormal activity can then be further investigated by security analysts to determine if it is malicious.

SIEM devices offer complementary services to IDS and IPS capabilities through their integration of data types. Not only do SIEMs offer a back-end platform to normalize and integrate the data, but they also offer front-end consoles or dashboards to provide a view of the integrated data for network and security operations staff analysis and response. This single view and access to data is intended to make it easier for security personnel to link IDS alert data to supporting information from log files [11].

Despite the advantages, there are areas where a SIEM device might not perform as well an IDS or IPS solution. Processing lag resulting from the methods by which a SIEM receives its data, for instance, prevents real-time action and alerting [10]. Data from logs are generally loaded into a SIEM in batches on a recurring schedule while alerts from IDS and IPS machines can stream in real time. This means that SIEM correlation of new log and alert data cannot occur until completion of a batch cycle. SIEMs may also have limitations in what data they can ingest from external devices, such as packet capture data that may not be available because of the significant storage requirements.

C. DATA STORAGE AND SEPARATION

Balancing access to various types of data and security of that data is a challenge for all network and security professionals. In order to be of use data must be accessible to the services, applications, and users that need it. That same data is also sought after by adversaries and threat actors, so it must be protected through a series of controls designed to achieve that balance. Two types of data are user data and mission data.

1. User Data

User data can be separated into to two separate categories. The first is user account information that represents the roles and responsibilities of network users. User account information contains data describing the rights of individual users to access the network and its applications, services and data. User account information must be secured from adversary actions, but must be made accessible in real time to the network services that consume the information as part of identity control and access management. The second category is data that specifically identifies the human being represented by the data. Personally Identifiable Information (PII) for most uses is limited to the account establishment process, but certain missions require the continued use of PII to support operations.

a. User Account Data

User account data is a centrally managed set of data that supports positive identification and enforcement of access control for an end user. Both Department of Defense (DOD) and Department of Homeland Security (DHS) use a two-factor authentication process to allow end users access to the core business networks. DOD requires users to use their government-issued common access card (CAC) and a PIN number to access computers connected to the Unclassified Nonsecure Internet Protocol Router Network (NIPRNET). DHS requires users to use their government-issued personal identity verification (PIV) card and a PIN number to access computers connected to the Unclassified Local

Access Network (known as LAN-A). Both DOD and DHS operate in this manner consistent with *Homeland Security Presidential Directive 12—Policy for Common Identification Standard for Federal Employees and Contractors* [13].

The combined use of the hard token (e.g., CAC or PIV card) and the PIN number is known as two-factor authentication. The card contains certificate information that allows the client computer system to call back to a central server (or virtualized and distributed set of services) that can verify that the card and PIN are matched to an authorized user account on the network. Each user session is discrete, in that users must re-authenticate themselves to start a new session or after a period of inactivity. The roles and access credentials stored in the central server follow the end user for their entire session and allow access to appropriate types of data, applications and services. The *Homeland Security Presidential Directive 12* requirement to comply with a two-factor authentication scheme, one of which must be a hard token, is an increased security measure over the simple username and password paradigms that persist in many networked systems and applications today [13].

Hard tokens are not yet fully implemented across the government for networks, applications or systems; and username and password systems are still in wide use. Systems with this level of user account information are especially inviting to threat actors, because the reduced security measures make it easier for adversaries to represent themselves to the network as authorized users to gain access. As such usernames and passwords should never be stored or transmitted together in plain text. One-way encryption or hash algorithms are typically used to protect username and password combinations, and password strength requirements are used to increase the password entropy to mitigate the threat of brute force cracking or guessing attacks. Access to the areas of the network where the user account information is stored should be heavily protected and extremely limited in access [14].

b. Personally Identifiable Information

PII is a class of data that can be used to specifically identify an individual. PII is frequently collected and stored as part of the human resource process and is used by the network as supporting information in account creation. There are also certain mission areas that require the collection and use of PII. These missions require the establishment of a system of record through a system of record notice (SORN) to comply with the Privacy Act of 1974, when any Federal agency creates a system that maintains records about an individual and those records are retrieved, indexed, or searchable by PII data. Examples of PII data include [15]:

- Names; full, maiden, mother's maiden, or alias
- Identification numbers; social security number, passport number, driver's license number, financial account or credit card numbers; numbers of personally owned property such as vehicle registration or title numbers.
- Address information; street or physical addresses and email
- Asset information; IP address or media access control (MAC) address that are statically assigned as a consistent link back to a person
- Telephone numbers; mobile and land, personal and business
- Personal characteristics: physical feature descriptions, photographs or images
- Information linked to the above; including date of birth, place of birth, race, religion.

2. Mission Data

Mission data (also referred to as business or operational data) represent the core data responsibility for protection and use and is integral to the responsibilities or value of the organization. This data is typically hosted on the internal network and is accessible through internal network applications or proxy services in the DMZ. Proxy services in the DMZ are responsible for ensuring that inbound requests are authorized and that query responses are compliant with the security polices of the network and organization. Figure 8 illustrates how a client machine first authenticates its user through account data, then supports access to mission data.

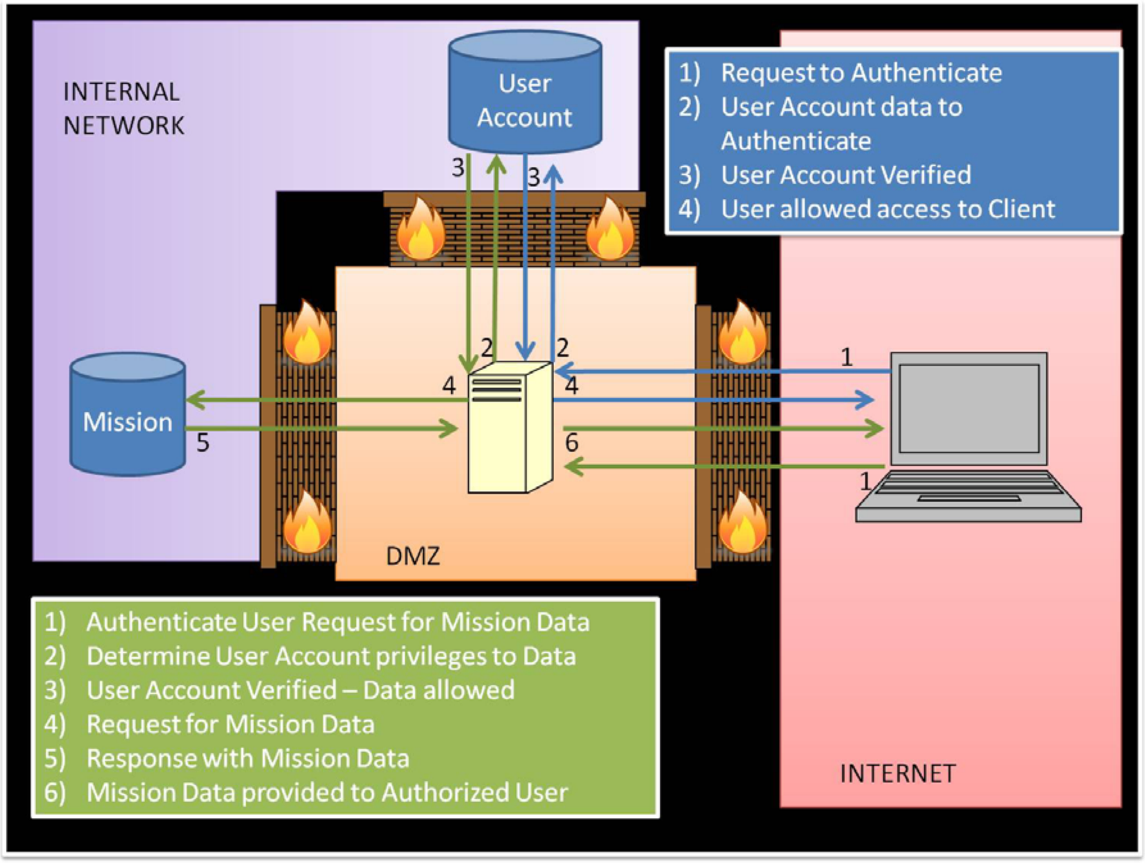
INTERNAL NETWORK
User Account
Mission
DMZ
INTERNET
1
2
3
4
5
6
1) Request to Authenticate
2) User Account data to Authenticate
3) User Account Verified
4) User allowed access to Client
1) Authenticate User Request for Mission Data
2) Determine User Account privileges to Data
3) User Account Verified – Data allowed
4) Request for Mission Data
5) Response with Mission Data
6) Mission Data provided to Authorized User

Figure 8. Simplified Access Request Process Illustration

D. ACADEMIC VIEW

All discussion in the chapter about network security principles has been based on or cited to federal or military publications governing the proper setup of secure networks. To ensure that the similarity of the respective military and law enforcement missions of the Departments of Defense and Homeland Security were not self-serving to this paper's intent to compare and contrast physical and cyber domains, additional research of non-federal entities was conducted to devise a list of requirements for network security. The network management and security requirements for the University of Massachusetts at Boston (UMB) were reviewed and chosen to serve as the representative source of non-military/law enforcement (LE) requirements. These network policies for the university were chosen because they were openly published in full detail and with traceability to the various laws created to protect actions on the Internet. The laws that are supported by the UMB network policies include, but are not limited to, the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, the United States Patriot Act and the Family Educational Rights and Privacy Act. The requirements for the network perimeter are as synthesized[1] as follows [16]:

- All inbound and real-time external connections are required to pass through an additional access control point (e.g., firewall). The access control point will uniquely identify each user, device, and port in use.
- All network traffic will be monitored as necessary to detect unauthorized activity or intrusion attempts and to ensure proper network management and performance.
- Security audits and scans of any computer, server, or network device may be conducted at any time to support network operations. If vulnerabilities that could jeopardize the larger network are identified, then corrective action will be taken, to include denying the subject machine access to the network until the problem is addressed.
- All network filtering devices must be approved by the network security group to ensure proper operation of the network.

E. CONCLUSION

This chapter reviewed the basic security concepts for network design. Purposeful creation of network perimeters through use of firewalls and DMZs separate sensitive networks from the World Wide Web. The National Institute for Standards and Technology (NIST) provides specific guidance on the implementation of monitoring technologies through intrusion detection and prevention platforms. The security design of the network must balance authorized use and access of necessary data against the protection from

[1] Not all requirements published by UMB are presented in this list, just the ones for the network security. The requirements listed were distilled to their core functions. The full list can be seen on the UMB website at www.umb.edu/it/policies/server.

unauthorized attempts to access that data. Security in network design is not just a concern for the federal government or military as seen in the network policies of the IT department at UMB. Chapter IV will discuss how the application of combat outpost security concepts to a CO discussed in Chapter II apply to the secure network concepts outlined in this chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INVESTIGATION AND COMPARISON OF PHYSICAL VERSUS CYBER

The previous chapters examined typical implementations for FOB and CO security and protected network security. This chapter will conduct a comparative analysis of both to identify conceptual similarities that might facilitate the transition of personnel from physical security roles in the military into the cybersecurity workforce.

A. MAPPING BETWEEN WORLDS

While a simple drawing like Figure 9 may serve to illustrate the idea that there is traceability between a physical location and a computer network in terms of security concepts, this section will provide details of how the two worlds are similar.

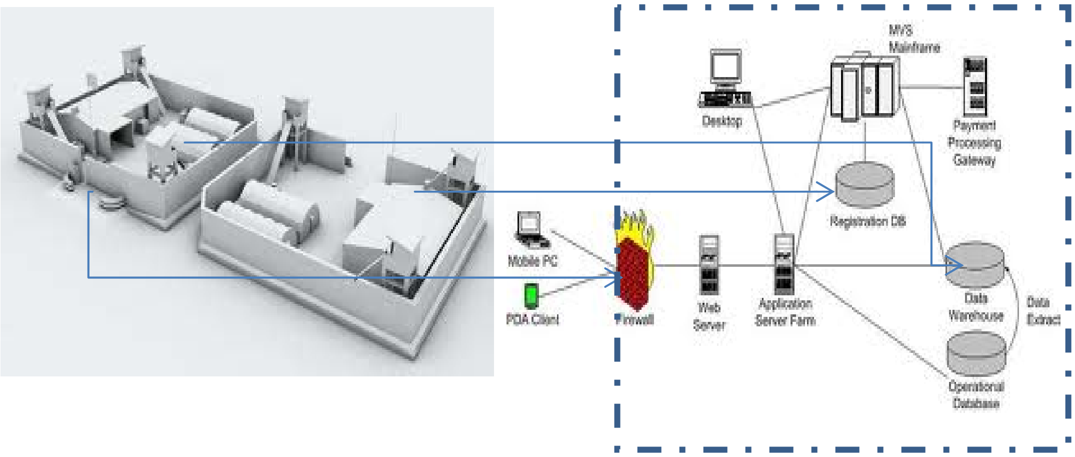

Figure 9. FOB and CO and Network Illustration

The mapping of military operations to cybersecurity concepts starts small with easily identifiable analogs. This primitive lexicon will serve as a foundation upon which advanced techniques and applications can be built in order to foster longevity and minimize miscommunication. Table 2 provides a cursory traceability of analog concepts between the physical security of FOBs and COs and that of networks.

Concept	Physical	Cyber
Demarcation of Defended Area	Perimeter structure	Network boundary
Ingress/Egress Inspection Point	Entry control points	Firewalls/DMZ
Monitoring (Unmanned)	Ground sensors, LRAS,	IDS/IPS/SIEM
Monitoring (Manned)	TOC, patrols	SOC/NOC, CERT
Places	Buildings/structures	Data storage
People	Living quarters/work quarters	Personnel/account data/PII
Things	Fuel/ammo supply areas	Mission data

Table 2. Cyber and Physical Security Concept Alignment

1. Similarities

Identifying the similarities between the physical and cyber worlds will serve to draw interest from warriors with combat experience looking for their next career highlighting facets of cyber security to which they can apply their skillsets.

a. Demarcation of Defended Area and Ingress/Egress Inspection Point

In a FOB or CO the perimeter is the lifeline for all soldiers to guard. It is watched vigilantly and protected ferociously. Nothing is supposed to enter or exit that perimeter without permission and protection. In a network the perimeter is the network boundary, used to demark ownership and responsibility. Security accreditation takes place within that boundary, and very tight controls are placed on the ingress and egress routes to and from the network enclave inside the boundary.

b. Monitoring (Unmanned)

For both physical facilities such as FOBs and COs and networked cyber systems, unmanned monitoring capabilities are comprised of sensors tied into systems that can interpret their data and make decisions based on rule sets. Unmanned capabilities can operate in a passive mode, where all data is collected and analyzed for presentation to a human for decision making, or they can operate in an active mode where responsive action is taken without human intervention. Physical systems such as the Combat Outpost and Force Protection System, also known as KRAKEN, have the ability to detect incoming enemy fire and return fire [17] just like the SAIC Cloudshield 4000 Deep Packet Processor can block, redirect, or modify malicious network traffic at line speed [18].

c. Monitoring (Manned)

Soldiers monitoring fusion cell displays and common operational pictures (COP) in a TOC perform the same role as network analysts monitoring a SIEM device in a NOC or SOC. In both areas sensors can produce large volumes of data that require automation to identify anomalies to present to humans for further investigation, however both areas also require skilled personnel trained in decision making, leadership, and technical expertise related to the systems and tools at their disposal.

d. Places

The careful and specific design of physical structures in a FOB or CO is a constantly evolving area of engineering. Physical structures must balance the logistical requirements necessary to build and maintain them with the mission requirements for adequate protection, capacity, and communications. Data storage requires the same exacting approach to design, engineering and execution. Capacity and access requirements must be well defined in support of the mission to enable proper and timely buildout of back-end data storage solutions.

e. People

The individuals stationed at a FOB or CO are there to accomplish a mission. They must be accounted for, provided protection, and assured that proper adherence to the rules will greatly increase their safety. User accounts for a network must be treated similarly. They represent the unique identity of a specific user. That identity is assigned specific roles and responsibilities on a network. The user accounts contain substantial PII and other sensitive information about the role that individual plays in the network. If user account information is compromised, then trust in the network erodes.

f. Things

Two important things for soldiers to locate and protect within a FOB or CO are the ammunition for the weapons and fuel for the vehicles and power generators. They both must be stored at minimum safe distances from where soldiers sleep, or where vehicles are parked in the event of an unintended detonation. Ammunition must also be easily accessed by soldiers in a fight. In a network, the business or mission data plays a similar role. It must be secured and protected from unwarranted access whilst being made readily available to proper access. Proper access to data must be met with timely and accurate delivery of the data without corruption or failure.

2. Differences

The differences in implementation of similar security concepts relates primarily to the manual nature of FOB and CO operations when compared with the potential for automation in a network environment. These implementation differences align with skillset gaps that will form the foundation for training in support of transitioning combat veterans into the cyber workforce.

a. Demarcation of Defended Area and Ingress/Egress Inspection Point

In the physical world the line of demarcation logically and physically encompasses the defended area. In the network sense, the definition is only logical. Networks are built around nodes (e.g., computers, switches, routers, etc.). Those nodes comprise the area, but there is not necessarily any physical space between them. Subsequently, the perimeter in a network sense is defined not by the physical location of the nodes, but by the paths by which external nodes can connect from outside the logical boundary. Individual nodes that cannot connect outside the boundary cannot even see the boundary.

Gates are used in a FOB or CO to specifically control the ingress and egress of individuals, vehicles, and equipment through the perimeter. It is very important for control to be established at these gates to allow for proper inspection, identification, verification and authorization for everyone and everything coming into the FOB or CO. Gates allow for throughput to be throttled or even stopped for a period of time in the event of a threat. Gates are a manual process for humans to administer thoroughly at a FOB or CO. In a network however, the security concepts for gates must be heavily automated. Firewalls and other boundary gateway devices are programmed with rules that control how internal and external nodes are allowed to communicate with nodes on the network. Access control lists (ACL), for instance, can be created to allow specific systems or applications to communicate across networks while limiting those communications to those that are required to conduct authorized transactions.

b. Monitoring (Unmanned)

Operationally and functionally, the unmanned capabilities in a FOB or CO and in the cyber domain are similar. An analysis and summary presentation of effectiveness requirements for intrusion detection systems is presented in

Section IV-B-1. The most significant difference lies in the training required to operate and maintain the very specific technologies employed in unmanned monitoring modes.

c. Monitoring (Manned)

Within a physical installation, guards are placed on the perimeter in sentry roles at the gates and observation posts along the boundary. Guards are put on frequent patrol both inside and outside the perimeter. They operate the gates and when required, the guns, in their role as protectors of the FOB or CO. Everyone in the FOB or CO is responsible for security, but those on guard at any specific time are required to be the most vigilant. NOC and SOC and Computer Emergency Readiness Team (CERT) operators provide similar functions but use very different methods. NOC and SOC operators have their eyes on the perimeter and the network assets. They are responsible for updating the ACLs inside the firewalls, updating the anti-virus (AV) signatures in use on host machines, and pouring through volumes of audit log data in search of anomalies that might indicate malicious activity. NOC and SOC operators rely on sophisticated SIEMs that automate much of the audit process. When malicious activity is identified, CERT operators are deployed to handle on-site response activities as a service to the compromised organization.

d. Places

Constructing physical structures can require large engineering teams and mechanical equipment. As an example of the amount of time required to construct a CO, recent requirements statements for future CO technologies have required that a CO be constructed in 30 days or less. COs are built in hostile environments as a means to support counterinsurgency or other operations. Data storage solutions, on the other hand, are part of a very mature commercial market space, with turn-key solutions available from a number of vendors. Supported by virtualization and cloud storage services, data management teams can rapidly deploy data storage systems that meet the defined mission requirements. On-site engineers may be required to install the hardware required to host the data storage solutions, but most configurations and setup work following the hardware installation can be accomplished remotely from the network operations center.

e. People

Individuals, specifically service members, located in a FOB or CO are all individually responsible for security operations. Platoons may operate in shifts with primary security responsibility shifting between groups during daily operations, however, if enemy contact occurs and all soldiers are ordered to "stand to," everyone is again responsible for security. In the cyber world, where the similarity relates to the individual's data, the responsibility to protect that data can be situationally dependent. Individuals are still primarily responsible for inputting their personal data into information systems, and individuals are responsible for security concepts such as password management and authorized use. Unlike the physical model, however, general users eventually have no role to play with the security of their data while at rest within an IT system. If an IT system is compromised and user data is corrupted or stolen, there is nothing a user can then do to re-secure the system. Individuals must then fall back on personal mitigation strategies such as identify theft protection and credit monitoring to ensure that their stolen data is not being used in criminal activity.

f. Things

Guns and ordnance, from small arms to heavy weapons, provide offensive capabilities to soldiers in a FOB or CO. These capabilities are necessary to repel an attack and defeat the enemy at close range and at distance as required. Small arms are assigned to each individual soldier, and most soldiers are responsible for multiple small arms while on duty. These small arms can be of multiple types, including standard battle rifles, machine guns, precision marksman rifles and many others. AV signatures are similar to small arms in that they are assigned at the lowest level of individual, but humans are not the targets or protected entities in a cyber fight. Individual computing systems such as desktop end clients, network and application servers, and all networking gear must be individually hardened to mitigate cyber threats. The IDS and IPS sensors monitor and act on network traffic, but defense in depth protection starts at the lowest level machine. Host machines are loaded with anti-virus capabilities that use signatures to identify and remove malicious code from their systems. These signatures can vary in capability from simple filename matching, to cryptographic hashing algorithms to complex combinations of several indicators at a time.

B. IDENTIFYING TRAINING GAPS

Section IV-A combines the security concepts of the physical and cyber worlds to show how their similarities may support a transition for veterans. The differences identified in the previous section make it clear that the preponderance of the training required to support the transition of military personnel with physical security roles to cybersecurity positions lies in the technologies and implementation of the security concepts rather than the concepts themselves. Further specificity of the training gaps can bring practical fidelity to the analysis. The following sections analyze the requirements for systems designed to support physical and cybersecurity missions, specifically in the unmanned monitoring concepts and the requirements for cyber network defenders as shown in federal agency job announcements.

1. Operational Requirements

DHS and DOD have formal processes for the acquisition of new technologies. These processes are quite similar to each other and follow best practices of systems engineering lifecycles. Governing documents exist in both Departments to codify the processes. For DHS implementation of these processes is governed by the Acquisition Management Directive MD-102 [19] and its appendices and DOD implementation is governed by DOD Directive 5000.01, The Defense Acquisition System and DOD Instruction 5000.2, *Operation of the Defense Acquisition System* [20]. Both processes require approval of a formal requirements document prior to committing funds to procure or build a new capability. Further, requirements documents are required to lay out the operational requirements of the mission that will be supported by the new capabilities. In DHS this document is the Operational Requirements Document (ORD) [19] . Capabilities Description Documents (CDD) are the DOD equivalent to the DHS ORD [19], [20].

Analysis of various ORDs and CDDs for both physical and cyber intrusion detection and prevention systems in DOD and DHS has led to this generalized list of measures of effectiveness (MOE) by which these systems can be assessed: [21]

1. Intrusion detection rate: The capability to detect a given percentage of attempted intrusions into a defined protected area
2. Error rate: The mathematical inverse of intrusion detection rate
3. Sensor communication: The sensors will communicate data in real time.
4. Sensor coverage: Sensors will have the capacity to sense intrusions in a specific maximum size area (physical systems) or across a specific maximum number of network nodes (cyber systems)
5. Adaptable coverage: User changes to sensor settings can be made with instant application of effect and maintain effectiveness within any range less than maximum.
6. Threat characterization: Sensors have the ability to distinguish threat types at intrusion.
7. False alarm rate: The rate at which friendly/allowed intrusions are characterized incorrectly as threat activity; Written as less than or equal to or not to exceed given percentages. False alarm may be a subset of Error rate.
8. Layered detection: Sensors must be able to distinguish between signs of a possible or impending intrusion versus occurrence of an actual intrusion.

Of these MOEs, intrusion detection and error rate highlight the need for sensor data to be highly accurate. The effectiveness of all downstream analysis of the sensor data is hindered if the high success rates are not met. NOC, SOC and CERT operators will need to be able to interpret and trust the sensor data as they execute their mission.

Requirements three through five highlight the need for intrusion detection and prevention systems to operate in real time and adapt to the dynamic nature of the monitored environment. As the nature of threats change to increase their chance of success, the security apparatus must also be ready to adapt. This implies that the apparatus must be able to detect threats in real time up to the maximum range or bandwidth of the protected system. Additionally, sensors must also communicate with the fusion center in real-time. In a cyber defense model, the fusion center is operated by NOC or SOC personnel who continually tune the sensors to maximize detection rates and ranges and continually adapt to the threat. In environments where smart sensors are able to tune themselves, the NOC and SOC operators must be able to interpret changes in the data stream that result from the sensor changes.

Requirements six through eight address the necessary skill sets of cyber professionals providing security, utilizing systems that meet all other requirements. Cyber warriors need to be able to distinguish good activity from bad activity, between different types of bad activity, and adjust to the subtle signs of changing activity in network operations. This need is anchored by fundamental skillsets in networking concepts such as channels, ports and protocols and their implementation and use in authorized and unauthorized network activity.

2. Outline Cyber Job Requirements

There is no single or dedicated federal General Series occupational category for cybersecurity professionals, but cybersecurity positions fall into a pool of different job specialties. The most prevalent job series is the information technology (IT) specialist, GS 2210. Another job series is the computer scientist, GS 1550 job series. The main difference between the job series is the positive education requirement in the GS 1550 qualifications which requires a college degree in computer science or computer engineering. IT specialists, on the other hand, have no positive education requirement [22].

Data was collected from job listings on the USAJobs website in the time period of February 15 through April 15, 2014. The job listings were of new federal job announcements in the 2210 and 1550 job series at the grade level of GS 9-11 (entry level) with key words “cyber” and “cybersecurity.” Results included 76 separate job announcements for vacancies across all three branches of government, multiple cabinet-level agencies in the Executive Branch, all four branches of military service, and multiple sub-agencies [23]. Unfortunately for this research, there was very little insight to be gained from the boilerplate language approved by the Office of Personnel Management (OPM) to advertise the knowledge, skills, and abilities required to perform these jobs. Research turned to the National Security Agency’s job announcements for cybersecurity jobs and found sufficient information to create a list of detailed requirements and technical competencies detailed in the remainder of this chapter [24], [25].

a. Position Requirements

Position requirements identify the necessary skills or tasks necessary to successfully perform the duties of the job. Position descriptions are an important method of communicating the needs of an organization in terms of human capital and helps job seekers to understand how their skillsets may apply to the job. The following list was assembled from reviewing multiple job announcements describing entry level cybersecurity positions in the federal government:

- Understanding of networking concepts, protocols, and implementations (e.g., TCP/IP, routing, DNS)
- Understanding of operating system concepts in both Windows and Solaris/Linux (e.g., processes and threads, file systems, memory) and proficiency in systems administration and command line tools.
- Hands-on experience managing, maintaining, troubleshooting, installing, and operating common operating systems and basic network infrastructure

- Understanding of and ability to describe current network technologies (e.g., routers, switches, firewalls)
- Experience with structured programming and scripting
- Understanding of common security solutions and their implementations (e.g., firewalls, intrusion detection systems, virus detection tools).

b. Technical Competencies

Technical competencies are detailed skills identified for specific jobs that describe the types of tools or technologies that applicants must be familiar with or fluent in to be considered for the advertised position. Technical competencies add a deeper level of detail to a job description and are aligned with the position requirements. The following list was assembled from reviewing multiple job announcements describing entry-level cybersecurity positions in the federal government:

- Operating system and network analysis
- Operating system administration (e.g., Windows and Unix or Linux)
- Intrusion detection and response
- Penetration testing
- Packet analysis
- Computer and network forensics
- Low level protocol analysis
- Network administration
- Vulnerability analysis
- Malicious code analysis
- Network applications
- Strong writing and verbal skills
- Networking protocols
- Log and packet-level tool experience
- Network attack techniques
- Operating system platforms (e.g., UNIX, Linux, Microsoft Windows)
- Network intrusion analysis and incident response

C. CONCLUSION

This chapter combines the analysis from Chapters II and III and creates a linkage between the physical and cyber worlds to support transition for veterans in combat roles to service in cyber roles. That linkage is carried further with the review of the state of federal job positions in cybersecurity and identification of the applicable cyber job skills. Table 3 provides a consolidated view of the traceability from security concepts through the topics of this chapter and sets the conditions for Chapter V to explore the programs available to support veterans interested in further service through federal employment and available training programs that can provide the technical competencies required for federal cybersecurity positions.

Concept	Physical	Cyber	Technical Gap (Job Skill/Technical Competency)
Demarcation of Defended Area	Perimeter Structure	Network Boundary	Understanding of networking concepts, protocols, and implementations. (e.g. TCP/IP, routing, DNS)
Ingress/Egress Inspection Point	Entry Control Points	Firewalls/DMZ	Understanding of and ability to describe current network technologies (e.g., routers, switches, firewalls) Understanding of common security solutions and their implementations (e.g. firewalls, intrusion detection systems, virus detection tools)
Monitoring (Unmanned)	Ground Sensors, LRAS,	IDS/IPS/SIEM	Vulnerability Analysis Intrusion detection and response
Monitoring (Manned)	TOC, Patrols	SOC/NOC, CERT	Operating system and network analysis Operating system administration (Windows and Unix/Linux) Intrusion detection and response Penetration testing Packet analysis Computer and network forensics Low level protocol analysis Network administration Vulnerability analysis Malicious code analysis
Places	Buildings/Structures	Data storage	Hands-on experience managing, maintaining, troubleshooting, installing, and operating common operating systems and basic network infrastructure.
People	Living Quarters/Work Quarters	Personnel/Account Data/PII	
Things	Fuel/Ammo Supply Areas	Mission Data	

Table 3. Traceability to Job Skills

V. IDENTIFICATION OF AVAILABLE TRAINING IN SUPPORT OF TRANSITION

This chapter provides a survey of available commercial training in the areas of network, computer, and cybersecurity from a variety of commercial and educational institutions that will allow for traceability to a series of classes customized to fill gaps outlined in Chapter IV.

A. PRIVATE INDUSTRY CERTIFICATION PROGRAMS

This section reviews several certifications offered by private organizations that are applicable to careers in cybersecurity. Each of these certifications is supported by training options that include classroom instruction or self-paced online instruction. The majority of the certifications are associated with the Computing Technology Industry Association (CompTIA). Other organizations such as the Global Information Assurance Certifications (GIAC) organization, the International Council of Electronic Commerce Consultants and the Information Systems Security Certification Consortium also offer well respected certification programs [26].

1. Computing Technology Industry Association (CompTIA)

a. A+

The A+ certification is designed for entry level computer technicians. There are two exams that must be passed to earn the A+ certification. The exams cover the basic principles of computer technology. The first exams covers the essentials of installing and configuring personal computers and related peripheral hardware as well as basic networking. The second exam covers knowledge gained through practical application of the computer skill sets tested in the first exam. Practical application knowledge includes installation and configuration of various operating systems and establishment of network connectivity to support file sharing, web browsing, and email capabilities. Mobile platform operating systems are also covered by the latest version of the A+

certification exams. The A+ certification is valid for three years from date of issuance, and a continuing education program has been established for A+ certified professionals to maintain their currency and certification.

b. Network+

Network+ is a certification awarded to IT professionals that have demonstrated competency through a formal exam in the area of networking. Network technicians must demonstrate that they understand network technologies and how to install and configure networking hardware. Exam topics include the Open Systems Interconnection reference model and the ports and protocols required to securely establish connections between computers and servers and peripheral devices. These skills are necessary for Local Area Network administration and management of connections to Wide Area Networks. The certification objectives continue to evolve to meet technologies advances. Recent updates to the exam include networking virtualization and security.

c. Server+

Server+ is the CompTIA certification specifically designed to qualify IT professionals for working on servers. Servers require specific knowledge on hardware and operating systems that perform very differently than the client machines covered in the A+ certification. The Server+ exam covers skills and knowledge in storage technologies such as redundant array of independent disks and multiple computer processing units required to administer the large machines that operate as servers. The exam also covers practical application knowledge such as disaster recovery and continuity of operations planning and design for servers. CompTIA recommends that IT professionals complete A+ certification prior to seeking Server+ certification.

d. Linux+

Linux+ is the CompTIA certification that measures the skills and knowledge necessary to excel as an entry level Linux administrator. There are two exams that support the certification, which has been bolstered by association with the Linux Professional Institute. The first exam is focused on certifying IT professional as having the necessary skills to install Linux systems and set up the Linux file system using the command line interface. The second exam covers detailed operation of Linux systems such as setting up system services and using shells and scripting for data management. User interfaces, systems security and networking of Linux systems are also covered by the second exam. The Linux+ certification focuses on the use of the Linux operating systems as a server operating system vice a client desktop operating system. This focuses the certification into areas such as package management for various Linux distributions and mounting file systems such as Network File Systems and Server Message Block/Common Internet File Systems.

e. Security+

The CompTIA Security+ certification is issued after successfully completing one exam. The exam is designed to validate that IT professionals have the knowledge and skills to manage risk in securing a computer network. The exam covers topics such as access control and identity management. Cryptography is also an important topic covered by the exam to ensure the encryption and decryption of sensitive information is appropriately handled for data at rest and in transit. The certification exam continues to evolve to handle security concerns brought on by emerging technology areas such as cloud computing and business practices such as “bring your own device” policies that enable personal computing devices to be securely used with the business network. Certified IT professionals obtaining the Security+ certification will have demonstrated an understanding of risk identification and mitigation for network based security attack and how to employ deterrent tactics as they counter network attacks and close vulnerabilities.

2. Other Organizations

a. GIAC Certified Intrusion Analyst (GCIA)

The GIAC organization created the Certified Intrusion Analyst certification to validate an analyst's ability to install and configure IDSs and monitor network traffic with those systems. Analysts must also demonstrate that they can interpret and analyze network traffic and log files presented by the IDS. Candidates that have passed the exam and earned the GIAC certification have demonstrated abilities in 17 separate objectives of intrusion detection [27].

b. EC-Council Network Security Administrator (ENSA)

The International Council of Electronic Commerce Consultants, or EC-Council, developed a certification specifically for Network Security Administrators. The focus of this certification is to view network security as a defensive operation. The certification promotes fundamental skills in analysis of external and internal network threats. Candidates for this certification must demonstrate the ability to develop security policies that protect vital business or mission data. Those policies are implemented through configuration of firewalls and anti-virus systems. Technical security skills are required for implementation of security policies, but are not the only focus of this certification. Operational Security, information security, and the interdependency between those two domains are a core component of the certification. This ensures that candidate IT professionals understand security and can apply it to their networked computer systems [28].

c. Certified Information Systems Security Professional (CISSP)

The Information Systems Security Certification Consortium created the CISSP certification as the baseline certification for information security. The CISSP certification exam tests a candidate's knowledge in 10 different domains:

- Access control
- Telecommunications and network security

- Information security governance and risk management
- Software development security
- Cryptography
- Security architecture and design
- Operations security
- Business continuity and disaster recovery planning
- Legal, regulations, investigations and compliance
- Physical (environmental) security

These 10 domains ensure that candidates understand the details of security architectures designed to protect the information and systems within the network boundary. Details of an institution’s information assets and the formation of policies and procedures are tested with respect to how IT network structures and data transmission and transportation formats are implemented to provide for confidentiality, integrity, and availability. Risk management skills are measured to ensure proper software and hardware system development is done with security built in to the foundation of the architecture. Business interests such as continuity of operations and disaster recovery are assessed along with the legal and regulatory aspects of the information security industry. The CISSP was recognized in 2013 as a top certification in IT by TechRepublic and IT Strategy News. The training required to achieve this certification provides for a solid foundation to an IT security career [29].

B. NON-PROFIT ORGANIZATION PROGRAMS

The Federal Information Technology Security Institute (FITSI) is a non-profit organization founded to provide role-based training and certification programs to federal IT workers. FITSI administers a cyber training program focused on a class of veterans known as wounded warriors. Wounded warriors are veterans who have experienced serious injuries resulting in an end to their military career. The FITSI Wounded Warrior program specifically defines the characteristics that make veterans ideal candidates for retraining as cybersecurity professionals. Two of the six characteristics identified by FITSI are the ability to be trained and the aptitude for tactics and strategy [30].

The FITSI Wounded Warrior program provides training in a variety of cybersecurity disciplines using many of the available commercial training programs identified in Section C. Figure 10 illustrates how the FITSI program builds cybersecurity professionals from the ground up. The program is designed to provide a common base of instruction up to a generalist level, and then supports further specialization from that point forwards.

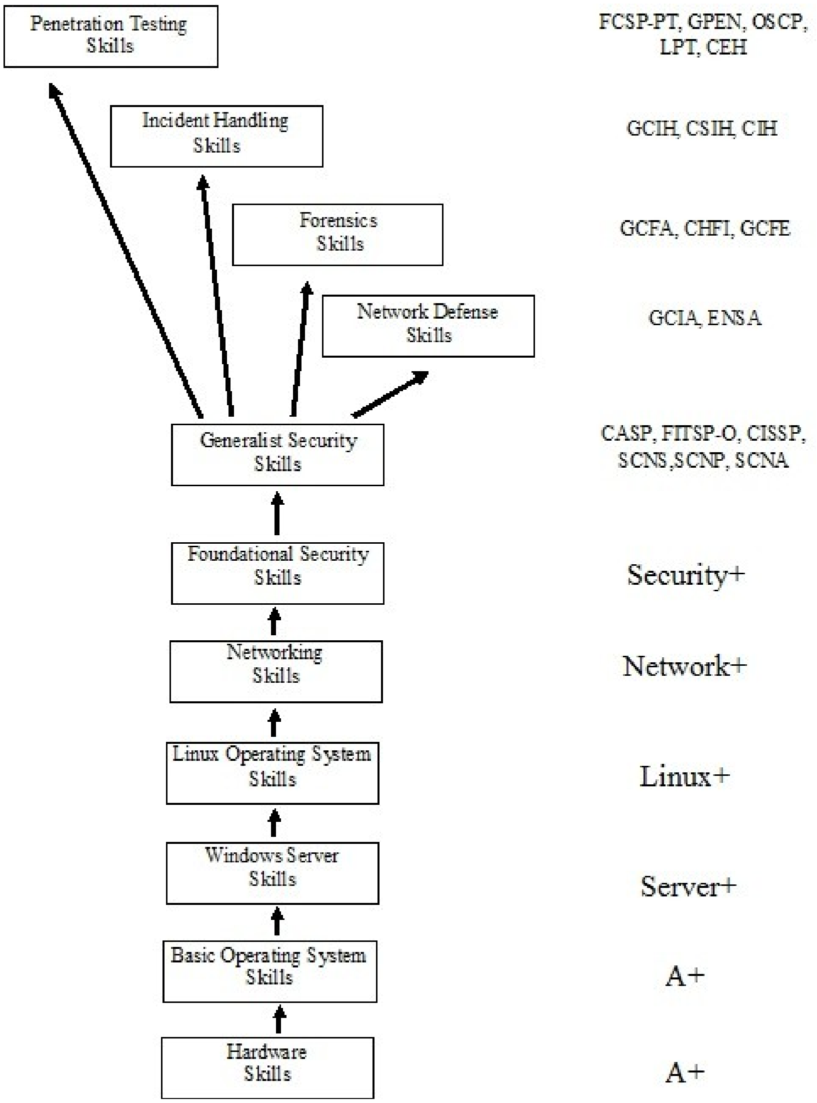
Penetration Testing Skills
FCSP-PT, GPEN, OSCP, LPT, CEH
Incident Handling Skills
GCIH, CSIH, CIH
Forensics Skills
GCFA, CHFI, GCFE
Network Defense Skills
GCIA, ENSA
Generalist Security Skills
CASP, FITSP-O, CISSP, SCNS,SCNP, SCNA
Foundational Security Skills
Security+
Networking Skills
Network+
Linux Operating System Skills
Linux+
Windows Server Skills
Server+
Basic Operating System Skills
A+
Hardware Skills
A+

Figure 10. Progressive Training Program, from [30]

C. FEDERAL EFFORTS IN CYBERSECURITY EDUCATION

1. Homeland Security Advisory Council Report

A 2012 Homeland Security Advisory Council (HSAC) report from the Cyberskills TaskForce provided eleven recommendations grouped under five Objectives to the Secretary for Homeland Security as follows: 1) ensure that the people given the responsibility for mission-critical cybersecurity roles and tasks at DHS have demonstrated that they have high proficiency in those areas; 2) help DHS employees develop and maintain advances in technical cybersecurity skills and render their working environment so supportive that qualified candidates will prefer to work at DHS; 3) radically expand the pipeline of highly qualified candidates for technical mission-critical jobs through innovative partnerships with community colleges, universities, organizers of cyber competitions, and other federal agencies; 4) focus the majority of DHS's near term efforts in cybersecurity hiring, training, and human capital development on ensuring that the Department builds a team of approximately 600 federal employees with mission-critical cybersecurity skills; and 5) establish a "Cyber Reserve" program to ensure the availability of a cadre of technically proficient cybersecurity professionals to be called upon if and when the nation needs them [31].

The third objective contains three of the eleven recommendations in the report. In the group of recommendations under Objective #3 is Recommendation #8, which calls for the Department to launch a major, sustained initiative to enhance the opportunities for U.S. veterans to be trained and hired in mission-critical cybersecurity jobs.

Recommendation #8 has eight implementation steps discussed in the report including outreach and communication programs, and partnerships between DHS and the Department of Veterans Affairs (VA) to increase awareness of the need for cybersecurity professionals. The partnership includes mirroring website content on DHS and VA web space. This is an important communication tool to veterans seeking information about cybersecurity jobs in the federal government.

2. National Initiative for Cybersecurity Education

National Initiative for Cybersecurity Education (NICE) is a national initiative led by NIST and supported by DHS, DoED, NSF, DOD and ODNI. NICE is comprised of four Components: awareness, education, workforce structure, and training and professional development. One major output from the NICE initiative is the National Cybersecurity Workforce Framework. The goal of the framework is to describe the work and workers required to establish a cybersecurity workforce that is agnostic of organizational ties. The Framework is designed to support public, private and academic cybersecurity workforce needs. The Framework is organized into seven categories with 31 specialty areas. The seven categories of the workforce framework are [32]:

1. Securely Provision—responsible for building the secure information systems
2. Operate & Maintain—responsible for support and administration of the secure information systems
3. Protect & Defend—responsible for analysis and mitigation of threats to IT systems and networks
4. Investigate—responsible for investigation cyber event of crimes
5. Collect & Operate—responsible for specialized operations and collection of information
6. Analyze—responsible for specialized analysis of cyber information to determine potential for use as intelligence
7. Oversight & Development—responsible for leadership, direction, or guidance to improve efficiency of cyber workforce

D. FEDERAL VETERAN HIRING PROGRAMS AND INFORMATION WEBSITES

There are several websites in the .gov and .mil domains that discuss post-service employment options for veterans. They contain all the information or links to the information necessary for veterans to make informed decisions about how to find education, training, and employment opportunities. Two websites that speak to veterans specifically about cybersecurity opportunities are the National Security Agency's public facing website and the DHS National Initiative for Cybersecurity Careers and Studies (NICCS) website.

1. NSA

The NSA website discusses the general benefits of VA career transition to federal service, including benefits, leave accrual, credit towards retirement for time served in uniform and veterans preference points applied to the federal hiring process. Table 4 gives the details of veterans preference eligibility categories and required documentation.

Eligibility Title	Eligibility Points	Document Required
Preference Eligible with no disability	5 Points	DD214
Preference Eligible with non-compensated disability rating less than 10%	10 Points	DD214, application for 10 pt Veterans' Preference, completed SF15 with supporting documentation
Preference Eligible with disability rating of at least 10% but less than 30%	10 Points	DD214, application for 10 pt Veterans' Preference, completed SF15 with supporting documentation
Preference Eligible with disability rating of 30% or more	10 Points	DD214, application for 10 pt Veterans' Preference, completed SF15 with supporting documentation
Derived Preference	10 Points	DD214, application for 10 pt Veterans' Preference, completed SF15 with supporting documentation

Table 4. Veteran's Preference Eligibility, from [33]

The website further describes general available career fields, the necessary qualifications, and provides resources for resume writing. There are also hyperlinks to open job announcements for entry-level positions. There are general references to the skills learned while serving in uniform, but no specific mention of what those skills are or how they apply to work in cybersecurity [33].

2. DHS

The DHS NICCS website for veterans provides external references for two categories of information. The Education section provides six separate sources of education for veterans, and the Career section provides eight separate resources for discovering employment opportunities. Both sections contain links to generalized information and links that very specifically discuss options tailored to cybersecurity education and roles [34].

E. CONCLUSION

This section discussed available options in the commercial sector for training programs and certifications in cybersecurity skills. There are programs designed to train cyber warriors to perform a variety of roles serving the cyber mission. Further, there are several initiatives administered by the federal government to inform the nation about the need for people willing to serve the nation in cybersecurity professional roles. Information is being jointly shared by DHS, NSA, and other federal executive branch departments and agencies in an effort to recruit talent. Veterans are targeted with specialized information related to the hiring process to become a civil servant. In the next chapter, this information will be combined with the previous three chapters into a recommendation for how the federal government could improve the information presented to veterans and potentially increase the effectiveness of the hiring initiatives.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INTEGRATED FRAMEWORK AND SUMMARY

After identification and examination of the contents of the preceding chapters, this chapter will thread all of the information together into a recommended training framework. This recommendation will include identification of partnerships amongst federal departments that can create a viable path from service in a combat role to employment in a cybersecurity career field.

A. CONNECT THE DOTS

Chapter II reviewed the security concepts employed by forward operating bases and combat outposts including exposition of doctrinal concepts through the real-world example of the CO Keating in Afghanistan. Chapter III discussed the security concepts of computer network security with examples from federal, military and academic sources. Chapter IV combined combat and cybersecurity by identifying basic security concepts that bridge the two domains and discussed how federal cyber positions are defined with specific skill sets. The skills required for those jobs were then traced to the cybersecurity roles in chapter three, and linked back to physical security concepts. Finally, Chapter V surveyed a number of available commercial certifications and training programs that can provide the technical skills necessary to begin a career as a cyber professional. Those skills are validated by attainment of the associated commercial certifications.

The first security concept from studying forward operating bases and combat outposts is the concept of Demarcation of the Defended Area. A perimeter is a simple structure used to outline the area of the base and provides protection in the form of physical shielding. Networked computer systems also employ perimeters in the form of network boundaries. IT professionals that are capable of building a network boundary are required to have detailed knowledge of networking concepts and their implementations via network protocols. The training required to attain the CompTIA Network+ certification will provide the technical skills necessary to establish a secure boundary for a computer network.

The second security concept discussed in Chapter II was a controlled ingress and egress inspection point to allow only approved traffic to enter and leave the forward operating base and combat outpost. Vehicles and personnel are inspected for explosives or contraband prior to accessing an entry control point. The rate of speed on approach to the entry control point may be physically restricted by serpentine barriers. Only after the inspection is complete is access granted through the entry control point and through the perimeter into the base. Firewalls provide similar functionality for a network boundary by only allowing certain types of network traffic into or through a network DMZ for use or inspection. IT professionals require specialized training to apply the security concept of controlled ingress and egress through establishment of a DMZ and configuration of firewalls. CompTIA certifications such as A+ and Security+ validate the necessary skills for configuring firewalls to serve as entry control points. Further training in Server+ and Linux+ validates the skills required to configure servers and maintain services inside a DMZ that provide secure access to data on the network.

The next two security concepts pertain to monitoring activity within and approaching the perimeter. Monitoring is achieved through manned and unmanned capabilities. The unmanned capabilities within the Combat Outpost scenario involve ground sensors placed outside the perimeter to detect movement and inform personnel inside the Tactical Operations Center. In some cases, sensors can be automatically linked to weapons systems that translate the sensor data into targeting data and engage the target to defeat it. Cybersecurity professionals, working in network operations centers and security operations centers employ intrusion detection systems and intrusion prevention systems that feed network data back to a security incident event manager. The security incident event manager can correlate the sensor data and provide preliminary analysis to the cybersecurity personnel who then decide what course of action to take in defense of the network. Intrusion prevention systems can automatically detect and defeat many network threats without specific human supervision. The skills required to configure unmanned monitoring systems for computer networks include the ability to conduct vulnerability analysis and to perform intrusion detection and response. These skills are taught as part of the training required to achieve the CompTIA Security+ certification.

Manned monitoring of a forward operating base or combat outpost relies on personnel in a tactical operations center constantly assessing the situation presented to them by the data from sensors, cameras, and information feeds. Patrols require personnel to physically patrol the perimeter or assigned area and assess any situations that occur in their area of responsibility. Network operations center and security operations center cybersecurity professionals face a similar challenge to constantly observe behavior on the network. They must be able to analyze the data presented to them via monitoring tools and take action to address anomalous behavior. These professionals require skills in a variety of computer analysis areas such as vulnerability, malicious code, low level protocol, and packet analysis. They must also be able to administer a network and the various operating systems of the machines hosted on that network. The skills required for a career in a network operations center or security operations center align with those required by certifications such as a CISSP, GCIA, or ENSA.

The final three security concepts are associated with what is being protected within the perimeter. Buildings within a perimeter on a forward operating bases and combat outposts can serve a variety of purposes, but all of them require balancing requirements for mission accomplishment against security requirements. Living quarters and work quarters (e.g., a tactical operations center) require protection from incoming attack but must also support timely access between facilities. Ammunition and fuel stores must also be protected from incoming attacks but must be located a minimum standoff distance from the living quarters to minimize the effect of unintentional detonation of the ammunition or fuel as well. Similar concepts are employed when designing and implementing secure networks. When data storage is required on a network, data access must be both available and secure. When that data involves personally identifiable information, it must be encrypted when stored. Mission data must also be protected in accordance with its sensitivity and usage. Cybersecurity professionals who support these tasks must have experience in managing and implementing common operating systems and network infrastructures. These skills can be trained and validated through attainment of several CompTIA certifications including A+, Server+, Linux+, and Security+.

This document establishes a framework to identify a transition path from combat to cybersecurity. The framework identifies the security concepts associated with forward deployed service at a forward operating base or combat outpost and provides evidence that they provide a solid security foundation that can translate to cybersecurity through a targeted training approach. Furthermore, the technical skills needed to fill the gap for veterans with this experience are readily available through commercial training and certifications. Table 5 is a consolidated reference for mapping the discussion of this document into one digest view.

Concept	Physical	Cyber	Job Skill	Training Source
Demarcation of Defended Area	Perimeter Structure	Network Boundary	Understanding of networking concepts, protocols, and implementations. (e.g. TCP/IP, routing, DNS, etc)	Network+
Ingress/Egress Inspection Point	Entry Control Points	Firewalls/DMZ	Understanding of and ability to describe current network technologies. (e.g. routers, switches, firewalls, etc) Understanding of common security solutions and their implementations (e.g. firewalls, intrusion detection systems, virus detection tools, etc)	A+ Server+ Linux+ Security +
Monitoring (Unmanned)	Ground Sensors, LRAS,	IDS/IPS/SIEM	Vulnerability Analysis Intrusion detection and response	Security+
Monitoring (Manned)	TOC, Patrols	SOC/NOC, CERT	Operating system and network analysis Operating system administration (Windows and Unix/Linux) Intrusion detection and response Penetration testing Packet analysis Computer and network forensics Low level protocol analysis Network administration	GCIA ENSA CISSP

Concept	**Physical**	**Cyber**	**Job Skill**	**Training Source**
			Vulnerability Analysis Malicious code analysis	
Places	Buildings/Structures	Data storage	Hands-on experience managing, maintaining, troubleshooting, installing, and operating common operating systems and basic network infrastructure.	A+ Server+ Linux+ Security +
People	Living Quarters/Work Quarters	Personnel/Account Data/PII		
Things	Fuel/Ammo Supply Areas	Mission Data		

Table 5. Full Concept Map from Security Concept to Relevant Cyber Training

B. WHERE TO NEXT?

There are several agencies within the executive branch of the federal government that can enable and benefit from an effective pipeline of veterans into the civilian workforce. NICE review of the framework proposed here can form the basis for establishing or improving partnerships amongst the DOD, VA, DOJ and DHS to strengthen career development programs that focus on veterans transitioning from active duty to federal service. Further research and pilot activities can be conducted to validate findings and incorporate this training into transition assistance programs for separating service members to educate them about available options in the cybersecurity mission space. Towards this end, a training program should be developed based on this material and delivered to a group of combat veterans. Pilot program subjects can be identified through polling to concentrate on those veterans most interested in cybersecurity or computer technology who also possess confidence in being able to perform cybersecurity work. Reconducting the poll at the conclusion of the training can provide quantitative and qualitative evidence of improvements in student potential for a cybersecurity careers after military service.

The DOD is primarily responsible for national defense and invests heavily in training its Soldiers, Sailors, Airmen, and Marines in the finest leadership, situational awareness, and technical training available. DOD has a large civilian workforce as well that operates side-by-side with military personnel, especially in the cyber area. In particular, DOD runs several large cyber oriented organizations such as the United States Cyber Command (USCYBERCOM) and Defense Cyber Crimes Center (DC3) that employ large military and civilian workforces.

The DHS is responsible for coordination of national resources in a time of emergency. DHS operates several cyber organizations, such as the National Cyber Coordination and Integration Center (NCICC) which is comprised of several elements including both the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Controls Systems Computer Emergency Response Team (ICS-CERT). DHS also operates the Homeland Security Investigations group, which is a law-enforcement agency responsible for areas of cyber crime focused on child exploitation. The U.S. Secret Service also operates under the DHS banner and is responsible for investigating cyber incidents related to its protective detail mission and financial crimes responsibilities (e.g., fraud).

The DOJ is responsible for law enforcement within the United States for cyber crimes. They prosecute all manner of computer crime in partnership with the rest of the government. Like the departments mentioned above, DOJ operates more than one organization in the cyber domain. The Computer Crime & Intellectual Property section (CCIPS) is responsible for implementing the department’s national strategies for combating computer crimes. The Federal Bureau of Investigation, on the other hand, has a cyber crime section that deals in key priority areas like computer and network intrusions, identity theft, and fraud.

The VA operates the nation’s programs to provide services for America’s veterans. America’s service men and women are entitled to a lifetime of care and benefits, including health, training, and education. The VA can be a conduit to extend any training program to this nation’s veterans who have already separated from military service and would be interested in entering civil service in cybersecurity roles. While the VA has an internal cybersecurity role through their own Network Operations Center and Security Operations Center (NOC/SOC) personnel, its role in this partnership centers around the dedicated access to veterans.

C. SUMMARY

Combat veterans deserve every opportunity to continue service or gain employment after their military careers. They may not see a computer- or technology-heavy career field as a viable option due to lack of technical skills in that area. Providing a path for veterans to see how their skill sets can be applied to cybersecurity along with a viable means to receive the training necessary in the technical areas they lack is an important step. The federal cyber workforce is growing at all levels and would benefit from an influx of talent that understands service to the nation and mission centric ideals.

LIST OF REFERENCES

[1] Department of the Army, *Tactics in Counterinsurgecy* (FM 3-24.2). Washington, DC: Department of the Army, 2009, Ch. 6.

[2] Department of the Army, *Operational Terms and Graphics* (FM 1-02). Washington, DC: Department of Army, 2004.

[3] Department of the Army, *Offense & Defense* (FM 3-90-1). Washington, DC: Headquarters, Department of Army, 2013.

[4] US Army Engineering Research and Development Center. Force protection—Basing TeCD 1a," in *Science, Technology & Requirements Forum*. Fort Leonard Wood, MO, 2012.

[5] J. Tapper, *The Outpost: An Untold Story of American Valor*. New York: Little, Brown and Company, 2012.

[6] US CENTCOM. (2011, June 6). "FOIA exhibits for COP Keating." [Online]. Available: https://www2.centcom.mil/sites/foia/rr/CENTCOM%20Regulation%20CCR%2025210/Forms/AllItems.aspx?RootFolder=%2Fsites%2Ffoia%2Frr%2FCENTCOM%20Regulation%20CCR%2025210%2FCOP%20Keating&FolderCTID=0x012000BDB53322B36BD84DA24AF0C8F8BCD011&View={7AED4B57-43F2-4B7D. [Accessed March 13, 2014].

[7] M. Rouse, L. Ewens, and H. Hoppe, 2007 "DMZ." [Online]. Available: http://searchsecurity.techtarget.com/definition/DMZ [Accessed March 10, 2014].

[8] A. S. Tanenbaum, *Computer Networks*, 5th ed, Boston: Prentice Hall, 2011.

[9] Microsoft, *Perimeter Firewall Design*. Redmond, WA, 2004.

[10] The Snort Project, *SNORT Users Manual 2.9.5*. Vienna, VA: Snort Project, 2013.

[11] K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems*. Gaithersburg, MD: National Institute of Standards and Technology, 2007.

[12] J. Brown, "Protect the network perimeter," McAfee, Santa Clara, CA, 2011.

[13] Executive Office of the President, *Homeland Security Presidential Directive 12*. Washington DC: Executive Office of the President, 2004.

[14] K. Scarfone and S. Murugiah, *Guide to Enterprise Password Management* (NIST SP 800-118). Gaithersburg, MD National Institute of Standards and Technology, 2009.

[15] E. McCallister, T. Grance and K. Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (NIST SP 800-122). Gaithersburg, MD: National Institute of Standards and Technology, 2010.

[16] UMass Boston, "Network Server Security Requirements & Procedures," UMass Boston, Boston, 2013.

[17] K. Osborn. (2011, August 31). "'Kraken' provides needed intelligence, force protection at NIE." [Online]. Available: http://www.army.mil/article/64655/_Kraken__provides_needed_intelligence__force_protection_at_NIE/. [Accessed March 29 2014].

[18] Leidos. (2014). "Cloudshield CS-4000 trusted network security platform," Leidos. [Online]. Available: http://www.cloudshield.com/products/platforms/cs-4000.asp. [Accessed April 28, 2014].

[19] Department of Homeland Security. (2010, January 21). *Acquisition Management Directive*. [Online]. Available: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_102-01_acquisition_management_directive.pdf. [Accessed February 28, 2014].

[20] Department of Defense. (2011, November 20). *Defense Acquisition System*. [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf. [Accessed February 24, 2014].

[21] DHS S&T. *Operational Requirement Document for Integrated Intrusion Prevention Systems*. Washington DC: DHS, 2010.

[22] National Initiative for Cybersecurity Education. *2012 Information Technology Workforce Assessment for Cybersecurity Summary Report*. DHS, Washington DC, 2013.

[23] USAJOBS. (2014, April 15). USAJOBS advanced search results. [Online]. Available: https://www.usajobs.gov/Search/GetAdvancedSearchResults. [Accessed April 15 2014].

[24] Department of Defense, “Job description—Intrusion Analyst Skill Development Program.” [Online]. Available: https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_JOB_DTL&Action=A&JobOpeningID=1037810&SiteId=1&PostingSeq=1. [Accessed April 14 2014].

[25] Department of Defense, “Job listing—Computer network operations operator.” [Online]. Available: https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_JOB_DTL&Action=A&JobOpeningID=1040178&SiteId=1&PostingSeq=1. [Accessed April 14 2014].

[26] CompTIA. (2013). “CompTIA certifications,” CompTIA, [Online]. Available: http://certification.comptia.org/getCertified/certifications.aspx. [Accessed April 27 2014].

[27] GIAC. (2014). “Intrusion analyst certification: GCIA,” GCIA. [Online]. Available: http://www.giac.org/certification/certified-intrusion-analyst-gcia. [Accessed 2 May 2014].

[28] EC-Council, “EC-Council network security administrator,” EC-Council, 2014. [Online]. Available: http://www.eccouncil.org/Certification/professional-series/ensa-course-outline. [Accessed 02 May 2014].

[29] International Systems Security Certification Consortium, “Certified Information Systems Security professional,” January 2014. [Online]. Available: https://www.isc2.org/uploadedFiles/Credentials_and_Certifcation/CISSP/CISSP-Information.pdf. [Accessed May 1, 2014].

[30] J. Wiggins, “W2CCA-Final,” 2012. [Online]. Available: http://www.w2cca.org/images/W2CCA-Final.pdf. [Accessed 05 Dec 2013].

[31] Homeland Security Advisory Council, “Cyber skills Task Force report,” Department of Homeland Security, Washington, DC, 2012.

[32] NIST, “NICE Framework,” Department of Commerce, 30 July 2013. [Online]. Available: http://csrc.nist.gov/nice/framework/ [Accessed April 30, 2014].

[33] National Security Agency. (2014, April). “NSA career opportunities for transitioning military.” [Online]. Available: http://www.nsa.gov/careers/opportunities_4_u/transitioning_military/index.shtml. [Accessed 2 May, 2014].

[34] Department of Homeland Security. (2014, March 13). “National Initiative for Cybersecurity Careers and Studies (NICCS).” [Online]. Available: http://niccs.us-cert.gov/home/about-niccs. [Accessed 02 May, 2014].

INITIAL DISTRIBUTION LIST

1. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

2. Defense Technical Information Center
   Ft. Belvoir, Virginia